

Nimsoft Service Desk

User Guide

Administrator

6.2.1



Legal Notices

Copyright © 2012 CA. All Rights Reserved.

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

Contact Nimsoft

For your convenience, Nimsoft provides a single site where you can access information about Nimsoft products.

At <http://support.nimsoft.com/>, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- Nimsoft Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about Nimsoft product documentation, you can send a message to support@nimsoft.com.

Contents

Contents	5

Chapter 1: Introduction	15

Overview	15
Features.....	15
Ticket Features	16
Non - Ticket Features	18
Structure of User Guide	21

Chapter 2: Key Concepts	22

ITSM/Global Concepts.....	22
Affected Services.....	22
Approval	23
Approval Groups	24
Categorization	24
Attributes	25
CI Relationships	26
Change Management.....	27
Configuration Management.....	29
Incident Management.....	31
Knowledge Management	33
License Type	34
Problem Management	35
Request Management.....	38
Roles.....	40
Service Desk Tickets	41
Service Feedback.....	42
Service Level Agreement.....	42
Service Level Management	44
Support Groups	45
Time Zones	46
Single Sign On.....	47
Ticket Related Concepts	47
Action Options	47
Auto-Routes	48
Case ID for Tickets	49

Categorization of Tickets.....	50
Global Issue	51
Prioritization.....	52
Task Groups & Task Flows.....	52
Task Management.....	55
Ticket Assignment	57
Ticket Custom Fields	57
Ticket Phase	58
Ticket Status and Reason Code	59
Ticket Relationships	60
Ticket Templates	61
Ticket Workflows	62
Work & Time Tracking.....	62
Request Handling Process.....	63
Special Function	64
Set Fields	65
Core Application Concepts	66
Communication Logs.....	66
Communication Templates	67
Dashboard Charts.....	68
Defined Searches	68
Emails Based Working.....	69
Global Search	69
Matching Conditions	70
Notification	71
Permissions	72
Primary Organization	72
PIN Authentication of Contact	73
Relationships.....	73
Reporting.....	74
Scheduled Hours & Holidays	75
Scheduled Activity.....	76
Self-Service User Interface	76
Configuration Parameters.....	77
Sort Order	78
VIP User.....	79

Chapter 3: Application Functionality 81

Introduction	81
Ticket Related Functionality	81
Non-Ticket Functionality	88

Frequently Asked Questions	97

Chapter 4: Access and Permission **99**

Overview	99
Manage Access	99
Manage Permissions	102
Organization Based Security	106
How Do I	119
Frequently Asked Questions	122

Chapter 5: Internationalization **123**

Overview	123
Approach	124
Setting User Locale	124
Searches	126
Enabling Translations	127
Localization of Email Communications	128
Assumptions and Intended Behavior	132
Known Limitations	134

Chapter 6: Layout and Navigation **136**

Overview	136
Layout	137
Navigation	144

Chapter 7: Administrative Modules **145**

Overview	145
Application Setup	145
Workflow Tools	154
Administration Utilities	159

Chapter 8: Manage Configuration **164**

Overview	164
Manage Configuration Actions	164
How Do I	177
Frequently Asked Questions	181

Chapter 9: Email Setup **182**

Overview	182
Setting up Email Functionality	182
Known Limitations and Workarounds	185
How Do I	186
Frequently Asked Questions	188

Chapter 10: Manage Organization **189**

Overview	189
Manage Organizations	189
Manage Organization Check points	193
How Do I	193
Frequently Asked Questions	197

Chapter 11: Manage Contacts **200**

Overview	200
Create and Modify Contact Records	200
Manage Application Related Information	203
Additional Information Tabs	204
Manage Contact Checkpoints	204
How Do I	205
Frequently Asked Questions	207

Chapter 12: Manage Support Group **212**

Overview	212
Create and Modify Support Group	213
Manage Support Group Business Hours	216
Manage Support Group Checkpoints	217
How Do I	218
Frequently Asked Questions	221

Chapter 13: Manage Roles **225**

Overview	225
Create and Modify Roles	225
Manage Role Relationships	226
Manage Roles Check Points:	226
How Do I	227
Frequently Asked Questions	228

Chapter 14: Manage Holidays	230
Overview	230
Create and Modify Holiday Groups.....	230
Manage Holidays Check points	231
How Do I	231
Frequently Asked Questions	232
 Chapter 15 - Manage Categorization	 234
Overview	234
Create Categorization Records.....	234
Manage Categorization Check points.....	235
How Do I	236
Frequently Asked Questions	237
 Chapter 16 – Bulk Process Data	 239
Overview	239
Manage Bulk Process	239
Steps to Bulk Process Data	240
Bulk Process Operations.....	241
How Do I	242
Frequently Asked Questions	242
 Chapter 17 – Manage Attributes	 245
Overview	245
Create and Modify Attributes	245
Manage Attributes Check points.....	246
How Do I	246
Frequently Asked Questions	248
 Chapter 18: Configuration Management	 250
Overview	250
CI Attribute Templates	251
Managing CI Records.....	252
CI Relationships	253
Administering Configuration Management	257
How Do I	259
Frequently Asked Questions	264

Chapter 19: Knowledge Management 270

Overview	270
Manage Knowledge Base Article	271
KB Article Category	272
Create KB Articles.....	273
Knowledge Management Functionality	275
Administering Knowledge Management.....	279
How Do I	281
Frequently Asked Questions	285

Chapter 20: Manage Ticket Modules 288

Overview	288
Setting Up Tickets.....	289
Ticket Custom Fields.....	293
Administering Ticket Functionality.....	296
How Do I	301
Frequently Asked Questions	306
Manage Value List	306
Manage Custom Fields	307

Chapter 21 - Manage Ticket Templates 310

Overview	310
Create Ticket Template	310
Manage Ticket Template Check Points	314
How Do I	315
Frequently Asked Questions	318

Chapter 22- Manage Task Group 321

Overview	321
Create Task Group.....	321
Manage Task Group Check Points.....	322
How Do I	323
Frequently Asked Questions	324

Chapter 23 – Manage Task Flow 326

Overview	326
Create Task Flow	326
Manage Task Flow Check points	328
How Do I	329

Frequently Asked Questions	330

Chapter 24- Manage Communication Template 332

Overview	332
Create or Modify Communication Templates	332
System Defined Communication Templates	337
Manage Communication Template Check points	337
How Do I	338
Frequently Asked Questions	342

Chapter 25- Manage Workflow Actions 346

Overview	346
Manage Workflow Action	347
Manage Action Options Check Point.....	356
How Do I	356
Frequently Asked Questions	362

Chapter 26- Manage Auto-Routes 366

Overview	366
Manage Auto-Routes	367
Manage Auto-Route Check Points	372
How Do I	373
Frequently Asked Questions	377

Chapter 27- Manage Approval Groups 381

Overview	381
Create or Modify Approval Groups	381
Add Approvers and Reviewers	383
Approval Types.....	386
Manage Approval Groups Check points	387
How Do I	388
Frequently Asked Questions	389

Chapter 28 – Service Level Management 393

Overview	393
Service Metrics	393
Service Targets	396
Manage SLA Monitoring.....	406

Manage Service Targets Check points.....	407
How Do I.....	407
Frequently Asked Questions	417

Chapter 29 – Service Feedback 419

Overview	419
Manage Feedback Forms	419
Manage Feedback Schedules	421
Review Feedback Results	424
Service Feedback Reports	424
Administering Service Feedback	424
Manage Service Feedback Check Points	426
How Do I.....	427
Frequently Asked Questions	430

Chapter 30 – Manage Schedules 434

Overview	434
Manage Schedules	434
Schedule Log	436
Manage Schedule Check points	437
How Do I.....	437
Frequently Asked Questions	439

Chapter 31 – Manage Defined Searches 441

Overview	441
Manage Defined Searches.....	441
Manage Defined Searches Check Points	443
How Do I.....	444
Frequently Asked Questions	445

Chapter 32 – Manage Charts 447

Overview	447
Manage Charts	447
Manage Charts Checkpoints.....	450
How Do I.....	450
Frequently Asked Questions	452

Chapter 33- Manage Dashboards	453
Overview	453
Manage Dashboards	453
Manage Dashboards Check Points	455
How Do I	456
Frequently Asked Questions	457
 Chapter 34 – Trends and Metrics	 459
Overview	459
Types of Reports.....	460
Manage Reports Permissions.....	479
How Do I	479
Frequently Asked Questions	481
 Chapter 35 – Manage Config Parameter	 483
Overview	483
Config Parameters.....	483
Frequently Asked Questions	567
 Chapter 36 – Administration Utilities	 568
Overview	568
Links and Actions.....	568
How Do I	579
Frequently Asked Questions	582
 Chapter 37: Glossary	 586
 Appendix A: Licensing Information	 614

Chapter 1: Introduction

As Application Administrator, you play a very crucial role in setting up Nimsoft Service Desk instance as per the needs of the Organization. The configurations managed by you enable Nimsoft Service Desk to serve as an effective tool for managing the IT Support needs of your organization.

This section introduces you to the range of features and functionality offered by the application, provides information on various the various forms in the administrative modules. This guide also contains step by step instructions for configuring the application for the Self-Service Users and Service Desk Agents.

To understand Nimsoft Service Desk features available to Self-Service Users you can read through the Self-Service User Guide. Similarly, to understand the functionality commonly made available to Service Desk Agents or Analysts and how they use the application, you can read through the Agent User Guide.

Overview

In your role as Application Administrator, you will interact with Nimsoft Service Desk extensively. There are two stages of administrator involvement with the application. The first stage is during the bootstrapping process, where you will be involved in configuring Nimsoft Service Desk application as a tool to manage your IT Support needs.

Once the application is available to the different users i.e. the Service Desk Agents and Self-Service Users, you will be involved in routine activities like assisting and supporting the needs of the users; and making updates to suit the changing needs of IT Support in your organization.

The section below lists the key features and functionality offered by the application. You can understand the feature and then configure Nimsoft Service Desk to exploit the feature to suit the IT support needs of your Organization.

Features

Nimsoft Service Desk is highly configurable; and allows you to manage and customize available features and functionality as per your organizational needs. The features identified below have been separated into Ticket related features and non-ticket related features for easy reading.

Ticket Features

This section explains all features that are applicable to tickets. While some features are available on specific ticket types, other features are generic to all tickets.

Features	Explanation
Ticket creation via email to Support	Ability for end-users to log a ticket by sending an email to the support mail ID. A ticket gets logged in the Nimsoft Service Desk and notification gets sent to the identified recipients. Attachments sent with the mail get related to the ticket as ticket attachments.
Email based action or update on ticket	Ability for end-users, Service Desk Agents, or other stakeholders of a ticket to update the ticket by sending an email response to an email notification from the ticket. The response gets attached to the existing ticket, and updates the ticket appropriately.
Auto-Route based on Email Subject	Ability to configure Auto Routes based on Email Subject. This facilitates effective assignment of Email based Tickets.
Multiple Email Addresses for Same Tenant	Ability to have multiple mail boxes for the same tenant, which can be used for routing as well as setting up a workflow action based on the Sent To email address for an incoming mail.
Automatic Email notifications	Ability to send out automatic email notifications to stakeholders on an action on ticket, based on configurations managed by the application administrator.
Common fields across all ticket types	All ticket forms have a common look and feel; with similar fields and tabs on the ticket. Fields specific to a ticket type are laid out to fit within a common layout.
Ticket Templates for quick ticket creation	Ability to configure Ticket Templates with pre-populated fields for common and standard requests. Access to ticket templates can be managed by enabling or disabling permissions.
Assign on Create action for Ticket Templates	Ability to configure Auto-Assign on Create action for Ticket Templates. This ensures assignment of a template based ticket to an appropriate support group for immediate action.
Override Auto Route for Ticket Template	Ability to configure action to override Auto-Route for Ticket Templates, to ensure appropriate assignment of tickets created using the template.
Task Group Templates for Task Tickets	Ability to configure Task Groups with multiple individual Task Templates grouped together in a specified Task Order. This enables identifying all tasks needed for a given request and making it available as one template.
Task Flows Templates for Task Tickets	Ability to configure Task Flows, with Task Group(s) and individual Task Templates to be fired in a predetermined flow based on the Task Order.
Action on Success and Action on Failure	Ability to configure actions on Success or Failure of each task in a Task Flow. Based on Success or Failure of a previous task, the task flow can be completed, aborted, or the failure point can be corrected and the Task Flow

	can be submitted again.
Communication Templates for tickets	Ability to configure Communication Templates for standardized communication from tickets; and control access to the templates via permissions. Communication templates can be used for manual and automatic notifications.
Send Mail Option on Ticket	Ability for Service Desk Agents working on a ticket to send an email to the requester and other stakeholders directly from the ticket.
Schedule email for future DateTime	Ability for Service Desk Agents working on a ticket to schedule an email to be sent from the ticket at a future date and time.
Custom Fields for Tickets	Ability to configure Custom Fields for soliciting specific additional information for a ticket. These Custom Fields can be grouped into sections and can be made available to Self-Service users and Service Desk Agents.
Auto-Route for Assignment	Ability to configure Auto-Routes based on matching conditions for automatic assignment of tickets to a specific support group.
Auto Routes for workflow actions	Ability to configure a workflow action to be triggered by an auto-route. This can include actions like creation of task tickets, deleting a ticket, etc.
Workflow controlled Action Options	Ability to configure workflow actions for moving a ticket through its life-cycle. Action Options available to the agent can be controlled by the workflow actions.
Approval Based Actions	Ability to configure Approval Groups for different type of Change Requests and setting up options for Action on Approval or Action on Rejection of a Change Request.
Multi-level approval process	Ability to configure Multi-Level Approval Process, where a ticket can be manually submitted for approval at multiple levels; or automatically moved from one approval cycle to another via choosing appropriate options for Action on Approval or Action on Rejection.
Fields marked as Required Fields	Ability to control which fields will be Required Fields for Self-Service Users web interface; and thus ensure required information is gathered when a ticket is submitted.
Modifiable Value list options on tickets	Ability to modify values options for fields like Impact, Severity, etc., as per the conventions of the organization.
Control Ticket Toolbar options	Ability to control access to ticket toolbar options by enabling or disabling permissions for individual contacts, support groups, or roles.
Tickets marked as Global Issue	Ability to allow Service Desk Agents to mark a ticket as Global Issue; and manage the Global Issue and tickets related to a Global Issue.
Related Tickets	Ability for Service Desk Agents to relate a ticket to one or more tickets; and keep track of related tickets from the Related Tickets Tab.
Related Configuration Items	Ability for Self-Service Users and Service Desk Agents to relate one or more Configuration Item to a ticket; and view relevant CI details where necessary from the Related CI Tab or section of the ticket.

Search Solutions from Ticket	Ability for Service Desk Agents to search for Solutions directly from a ticket; and apply solution from available Knowledge Article that is likely to resolve the issue for updating Cause and Resolution details.
SLA Monitoring on tickets	Ability to enable or disable Service Level Agreement monitoring on tickets and ability to configure SLA targets for tickets.
Upload Attachment to Ticket	Ability for Service Desk Agents and Self-Service Users to upload an attachment to a ticket and keep track of the related attachment from the Attachments tab or section of the ticket.
Work log and time tracking	Ability for Service Desk Agents and Self-Service Users to update a worklog on a ticket; and for Service Desk Agents to log time spent on an activity in the worklog section of the ticket.
Activity Tab on tickets	Ability to view details of all actions on the ticket, including automatic actions and notifications and manual actions and communications in the Activity Tab. Service Desk Agents can also view Activity of related tickets.
Locked Tickets	Ability to lock and unlock tickets. Ticket being modified by another logged in user gets locked automatically and cannot be modified. Tickets can also be locked when submitted for approval.
Print Tickets Option	Ability for Service Desk Agents and Self-Service Users to print a ticket.
Export Ticket List as CSV/PDF	Ability for Service Desk Agents and Self-Service Users to export ticket list, search results output, etc. as CSV or PDF documents.

Some of these features can be enabled or disabled. To enable or disable a feature identified above, you can manage Configuration Parameters related to the feature stated.

Non - Ticket Features

The features explained below are available to enhance working with the tickets, and are available as a support to the ticket related features. Most of the features listed are configurable and you can modify them as per the IT Support needs of your organization.

Features	Explanation
Email notifications	Ability to send out email notification from the application. This includes notifications related to the ticket as well as notification for Service Feedback, Password Reset, etc.
Direct URL Links	Ability to provide Direct URL Link in email notifications. These Direct URL Links allow access to the application without separate user authentication.
AD Sync	Ability to run Contact Sync Software Program to periodically match contacts in your Active Directory with Nimsoft Service Desk contact records. New contacts from the Active Directory or similar programs are automatically added and contacts not listed are set as inactive.

Single Sign on	Ability to enable access the application directly without updating user name and password separately once a user has been authenticated into the system using single sign on.
Locale Selection	Ability for users to choose the language in which the UI is available by setting their own locale preference. Administrators can define a default locale for all customers.
Bulk Process of Data	Ability to bulk process (import and/or update and also delete) data related to Organization, Site and Location as well as Configuration Item records. Data can be gathered in an appropriate format and bulk uploaded.
Data Exports	Ability to export data listed in searches, ticket lists, etc. into CSV or PDF files. This includes data from ticket lists, Configuration Item lists, Knowledge Article list, etc.
Permissions to control access	Ability to control access to a ticket module or action link, access to communication and Ticket Templates, etc., to specific individuals or support groups via permissions. This is achieved through Managing Navigation Menus, Ticket Toolbar, Report configurations, etc.
Hierarchical inheritance of permissions	Ability to manage permissions in a hierarchical manner. Permissions can be given via a Role and/or Support Group to all Contacts related to the Role or Support Group.
Status of Entities	Ability to control access to an entity by managing the Status of the entity. When an Organizations made inactive, all site and locations below it and all related contacts automatically become inactive.
Reports	Ability to access a wide range of out-of-the-box Reports. These reports can be related to all Ticket Types, Configuration Items, Knowledge Article and Service Feedback Surveys.
Searches	Ability to search for records across the application. The Global Search Features allows search for entities across a range of modules; while Advanced Searches allow searches within each module.
Pre-defined Search	Ability to access a variety of Defined Searches; and the ability to configure new Defined Searches. Access to a defined search can be managed via permissions.
Personal Searches	Ability for Agent, analysts and administrators to create and save their own searches related to Tickets and Configuration Items. Personal Searches can be created and saved by the logged in user (Agent or Admin user) for their own use. They are available only to the logged in user who has created and saved the record and is not automatically shared with other users or controlled by permissions.
Dashboards and Charts	Ability to access a variety of Dashboards and Charts for all ticket types and Configuration Items. New charts and dashboards can also be configured and made available to different users.
CCTI based Categorization	Ability to apply categorization for Tickets, Configuration Items, and

	Knowledge Articles. Tickets and Configuration Items can be categorized at four levels based on Class, Category, Type, and Item.
Configuration Management Module	Ability to manage and maintain Configuration Item Records in a centralized Configuration Management Module. Ability to relate Configuration Items in different Relationship Domains and also view CI relationship graphs.
Knowledge Management Module	Ability to manage and maintain a Knowledge Base of solutions to issues, response to queries, and other informative articles. Access to Knowledge Base Articles can be managed via permissions.
Service Feedback Surveys	Ability to create Service Feedback Surveys and send out the surveys as per a feedback schedule.
Soliciting Anonymous Feedback	Ability to create Anonymous Surveys where the respondent can reply to a Service Feedback Survey anonymously.
Schedules for routine operations	Ability to configure schedules for routine operational activities. Tickets will be created as per the schedule and assigned to the identified individual or group for execution of the scheduled task.
Schedules and Holidays	Ability to associate schedules like working hours and holiday lists with Support Groups, Auto-Route, Service Availability, etc.
VIP Users	Ability to designate users as VIP Users. A message alerting the Service Desk Agents that the Requester or Requested for individual is a VIP User will be displayed to help prioritize the ticket accordingly.
User PIN Authentication	Ability to associate an authentication PIN for all contacts. This assists in activities where contact authentication could be required.
Notification diverted to Deputy	Ability for all contacts to raise an Out of Office flag; and divert notifications from the application to a deputy designated as alternate contact. This can be done directly by the logged-in user.
Filters for all lists	Ability to filter all lists visible across all forms. This is available for Service Desk Ticket related forms as well as forms in the Administrative modules.
System-Defined Communication Templates	Ability to access and manage system-defined Communication Templates to be used for automatic and manual notifications from the application.
Configuration Parameters	Ability to enable or disable a range of features and functionality via Configuration Parameters. These parameters control features for both Self-Service Users and Service Desk Agents.
Communication History	Ability to view and manage Communication History. A history of all communication sent and received by the application is available to the administrator.

To enable or disable a feature, you can modify and manage a related Configuration Parameter.

Structure of User Guide

The Administrative Modules of Nimsoft Service Desk are Application Setup, Workflow Tools, and Admin Utilities. The modules on Configuration Management, Knowledge Management, Service Feedback and Service Level Management also require to be setup by the administrator, as per the needs of the organization.

The Section on **Application Functionality** presents a comparative view of how particular application functionality is used by Self-Service Users, Service Desk Agents, and Application Administrators. **The Administrative Module** section gives a generic view of all forms and sections under the three Administrative Modules and the function of each link.

The chapters in this guide have been laid out to reflect the logical configuration sequence that could be followed when configuring Nimsoft Service Desk for the first time. Some of the items may not be in the same order in the Navigation Menu of the application.

The features and functionality of Nimsoft Service Desk can be tweaked to fit your specific requirement by enabling or disabling a specific Config Parameter. You can manage defaults that need to be applied to your instance of the application by setting appropriate value in the related Config Parameter. The section **on Manage Config Parameter** lists all Config Parameters and the value or functionality controlled by the parameter.

Each section contains detailed explanation about the administrative form used for configuring the feature or functionality, and information on correlation between various fields. Checkpoints while configuring an entity or record, detailed steps for configuring the record, and Frequently Asked Questions related to that section are contained within each section

A detailed glossary of terms, as applied to the application is contained in the Glossary section, for reference to the use of a term in the context of the application.

Chapter 2: Key Concepts

The design of Nimsoft Service Desk and the implementation of its features and functionality are guided by some key concepts. Being aware of these key concepts and how they are applied in Nimsoft Service Desk will enable you to explore the features and functionality of Nimsoft Service Desk fully.

Key Concepts are categorized into three groups, as seen below:

ITSM/Global Concepts

Affected Services

IT Infrastructure in an organization consists of Configuration Items. This could be hardware, software, networking devices, documentation, etc. Configuration Item related records, with details of various attributes of the record, can be maintained in the Configuration Management Database. Configuration Items can also be categorized as appropriate.

A Configuration Item contributes towards delivering a service or enabling the user to achieve a business goal. While in some cases an individual Configuration Item in itself is capable of delivering a business goal, usually several related Configuration Items are grouped together to deliver the business goal.

For better management of all configuration items that work together to deliver a business service, these related Configuration Items can be categorized under appropriate classifications and grouped together as a Service. You can also relate configuration items which work together to deliver the service in different relationship domains. This relationship can be seen by the relationship diagram. When an incident is related to a Configuration Item, the CI can be related to the ticket for better managing the incident.

Where a ticket is logged for reporting an issue on a CI classified as a Service, this information can be updated into the Affected Service section of the ticket. SLA monitoring can set up to monitor the downtime of the service and the time needed to restore the service can be managed accordingly..

Approval

ITIL recommends that all change requests to move through a Change Approval Process wherein the proposed change is thoroughly analyzed, its impact assessed, and its need validated and justified. This is done to ensure that the proposed benefits of the change are valid, and the change, if needed, can be implemented with minimal risk.

Nimsoft Service Desk allows the administrator to set up a change approval process for requests that need approval. Change Tickets get assigned to an Approval Group such as General Approval Groups or specialized approval groups that are set up.

A change once approved, can then be assigned to a competent group/individual for implementation of the change.

Self-Service Users, Agents, or Administrators can participate in the Change Approval process if they are associated with a ticket as a member of an Approval or Review Group. They can also be manually added to a ticket as an Approver or Reviewer. Approvers can either approve or reject a ticket. They can also defer the decision and ask for more information. Reviewers can only comment upon a proposed change.

Both Self-Service User interface and Agent's interface provide a list of changes assigned to a contact for Approval Or Review. They also receive Email notifications. The list of pending approvals permits a user to drill down to view details of the Change before making the decision.

Nimsoft Service Desk also allows for a multi-level approval cycle, wherein a change can be moved through multiple approvals before it is considered finally approved and can be taken further.

The Application Administrator can also configure options in a change approval process:

- All must approve
- Any One must approve
- Any One must approve or reject

In "All" must approve situation, the approval process ends if any one approver rejects the change proposal. Even if one approver rejects the proposal, the change is rejected. In other words, only if all approvers approve, proposal is approved.

In "Any One" must approve, the approval is approved as soon as any one approver approves and the approval is rejected only when all approvers reject the proposal.

In "Any One must Approve or Reject", the change approval is approved or rejected as soon as an approver approves or rejects the change. Thus, the decision of the first approver to "Approve" or "Reject" is applied to the change request. In this case, the Approval process does not wait for inputs from the remaining approvers.

Approval Groups

ITIL recommends that all Change request pass through an Approval Process. The approval process involves submitting the change request for review and approval to competent resources that can review the change request and approve or reject the change.

In order to facilitate the change approval process and to identify users who can participate in the approval process as Approvers or Reviewers of a change, you can configure approval groups. An Approval Group consists of individuals who are considered to be qualified to consider the request for change, study the implications of the change, and determine whether the change can be executed or not.

Configuring Approval Group allows you to bring together all individuals who can comment on a change together into one support group. An approval group will get associated with the change ticket based on the categorization (CCTI) applied to the ticket or other matching conditions specified in the Approval Group record.

Approval Groups can be configured for different types of change (standard, normal, break-fix, emergency, etc.), based on ticket CCTI, requester, etc. Approvers can also be picked contextually from the ticket, for example, Requester's Manager.

By configuring approval groups, you can facilitate the implementation of an effective change management process.

Categorization

Categorization is the process of logically grouping objects and entities for a specific purpose. Categorization provides a means of recognizing objects, differentiating them, and understanding them via similarities and differences in the context of their use.

Nimsoft Service Desk allows a four level hierarchical categorization - at the Class, Category, Type, and Item (CCTI) level. Categorization can be applied to Tickets, Configuration Items and Solutions in the Knowledge base. A class can have several categories under it, each category could further have several types, and each type can have several items.

For example, if the Class of a Configuration Item (CI) is Printer, the Category could be Laser, Ink jet, Industrial, or Dot Matrix. Further, a Laser printer could have Type as Epson, HP, Coolpix, etc., and the Item for HP could be 1100 i, 1120 p, etc. Such categorization of Configuration Items enables a structured way of maintaining records and assists in understanding of what is affected if there is an issue with the CI.

Similar categorization can also be used for tickets. For example a Ticket can have Class as Hardware, Category- Desktop, Laptop, Palmtop, Type, HP, Dell, HCL, Sony, etc. Such categorization applied to tickets facilitates effective auto-routing of tickets to appropriate support groups and enhanced ticket solution search; and thus a more effective management of the support related activity.

Note: An Organization must choose its scheme of CCTI very carefully with a long term perspective because, once a set of CCTIs are created and linked to CIs, Solutions, Workflow entities, tickets, etc., large scale redoing requires unlinking the relationships and reestablishing them.

Some of these tasks cannot be done through GUI. Nimsoft Service Desk Support will have to carry out the changes selectively through back-end.

Attributes

An attribute defines one specific property of an object, element, or file. Generally, objects have multiple attributes; and usually all attributes of the object are captured to gather adequate information about the object. Typically an Attribute consists of a name, its value, and units. Attribute values and units are generally variable.

Let us consider the example of a Configuration Items having CCTI class of "Switches". Switches would have several specific attributes such as, make, model, manufacturer, number of ports, capacity, etc. Each attribute helps detail one specific aspect of the Switch. Several such attributes collectively describe the CI - Switches.

A configuration Item record form has a range of standard attributes that are applicable for all types of configuration items. All attributes that help to specify a CI appropriately can be created as a Template and values can be captured for Individual CI of the group. The application administrator can add more attributes by configuring a CI Attribute Template and relating it to different CCTIs for configuration Items.

The various fields on a Ticket form which are used to capture specific information about the ticket are the Attributes of the Ticket. Some attributes on a standard ticket form are Priority, Severity, Impact, etc. These fields are used to gather specific information about the ticket.

Besides the standard fields, additional attributes can be added to the ticket in the form of Custom Fields on tickets. These fields on a ticket, which are used to capture additional information and to bring more detailed specifications are Attributes on a Ticket form.

Custom Field Templates can be created for Tickets, with specific attributes (and corresponding values) for a specific ticket type or a ticket with specific CCTI. This enables adding attributes to capture relevant information for more appropriate processing of a ticket.

CI Relationships

Configuration Items such as hardware, software, network devices, etc are managed by the IT Support and Service Provider. Usually, a set of related configuration items interact and work together to enable the user to achieve business goals supported by IT.

A configuration item is normally related to other entities within IT Services and Support, which includes:

- Relationships with other configuration items
- Relationship with contacts or users
- Relationships with tickets

You can maintain relationships of Configuration Items in Nimsoft Service Desk records.

A Configuration Item can be related to other Configuration Items in various relationship domains such as Power, Logical, Network, or Service. Based on the relationship domain, you can specify the relationship type between the related CIs. You can further classify a Relationship type to qualify the relationship.

For example, if one CI (A Server) is related to another CI (a UPS System) in a Power relationship, the relationship type could be specified as Receives from/Supplies to/Related to. This relationship within on relationship domain can be seen as a relationship diagram on the CI record.

You can relate a Configuration Item to contact records such as owner, user, change approver, change reviewer, or support provider. Relating a CI to a contact allows the contact to view and relate the CI to tickets created as appropriate.

If a ticket reported is for a Configuration Item or due to a Configuration Item, the Configuration Item can be related to the ticket. Establishing this relationship helps when working to solve the request. It also helps provide historical data about the Configuration Management, which can be used in case of a larger issue with the CI.

Change Management

Change is defined as Addition, Modification, or Removal of anything involved in delivery and support of an existing IT Service. This can include Configuration Items, application software, system software, configurations, access, permissions, or documentation.

A Change could be reactive - caused by occurrence of a Problem in the existing IT Infrastructure or service; or it could be proactive - aimed at improving or enhancing efficiencies of existing IT Infrastructure or service. In order to ensure that all changes are well planned and approved, Change Management comes into play.

The objective of Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes. As the rate of change in technologies and the associated need for change in the IT Service Offerings is mounting, changes that are not well planned can lead to problems. Therefore there is a need for tightly managed and controlled approach towards Change.

Change Management aims to minimize any undesirable disruptions to an existing IT Service due to Change implementation.

Change Management can be implemented through the Change Management Module of Nimsoft Service Desk. Configuration of Change Management process for an organization by Administrator requires configuration of Approval Groups and appropriate Workflow Actions to initiate and conclude approval decision process before implementation of the Change.

Change Management is the process responsible for ensuring that:

- Standardized methods and procedures are used for efficient and prompt handling of all changes
- All changes to service assets and Configuration Items are recorded in the Configuration Management System
- Overall business risk is minimized

Change Ticket Life-cycle

A proposed change typically passes through four phases which involve:

Phase 1: Raise Change, Capture detail of proposed change

Phase 2: Evaluate Change and record analysis of Risks, impacts on CIs, Services, Environments, etc., and plan details for implementation verification, contingency of back out, etc. "Submit for Approval" action to initiate Approval cycle

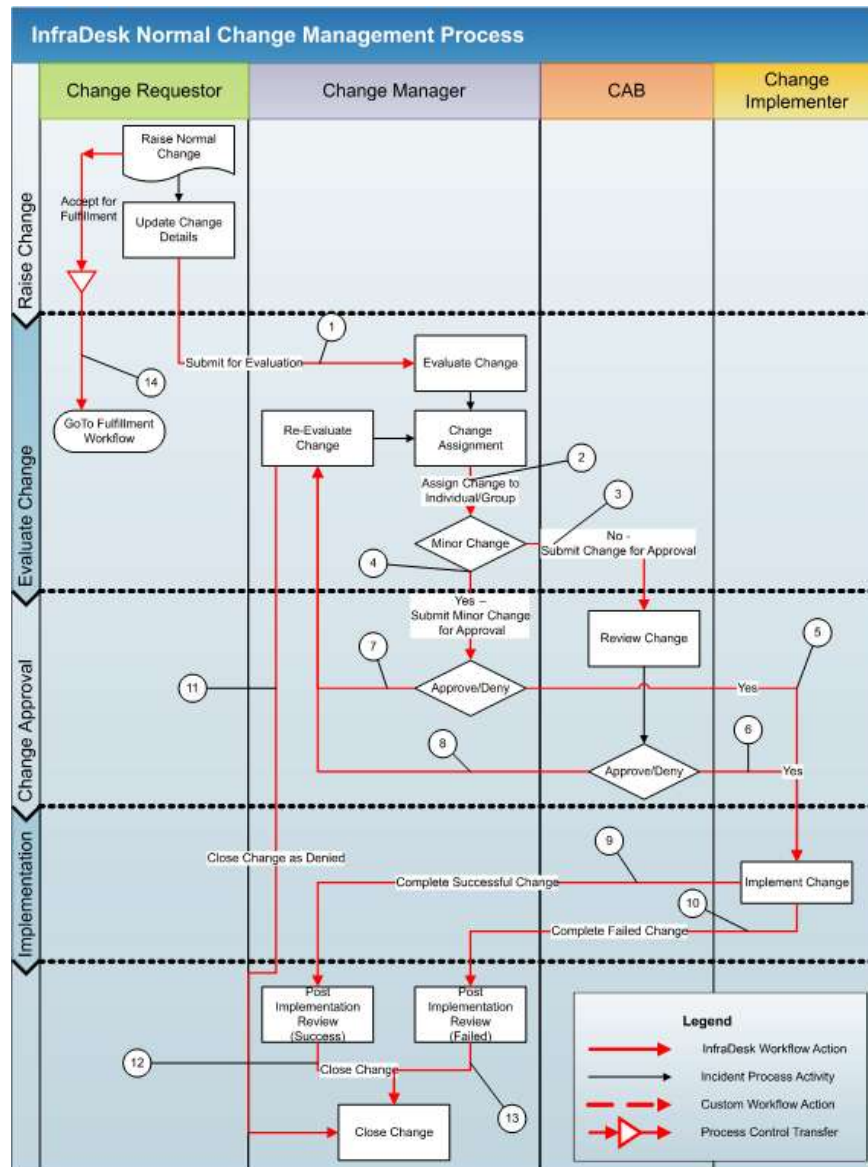
Phase 3: Approval or Rejection or Requests for more information by Approver / Reviewers

Phase 4: Implementation and verification of change. Action on successful implementation / Action on failed change

Phase 5: Change Post Implementation Review and closure

Change Management in Nimsoft Service Desk

The Change Management Module of Nimsoft Service Desk can be used to provide workflow automation for Approval and submission of Change Tickets. The default Nimsoft Service Desk Workflow for Management of Normal changes is depicted below.



As application administrator, you can configure a workflow that is different from the one seen above according to the processes and practices specific to your organization. Other workflows that apply specifically to Emergency changes and Child Change Tickets based on Service Requests that need approval and then revert to Service Request Fulfillment can also be configured.

Change Management Features

The following features are available to be used to manage the Change process:

- Ticket Templates for standard pre-approved changes and corresponding Task ticket templates
- More Detailed Information Tab to capture details applicable only to Change Management
- Displaying a Forward schedule of Changes in a Calendar
- Configuration of Alternative Workflow based on Change Type such as Normal, Standard, Emergency, or Break Fix
- Configuration of alternative workflows for Major versus Minor Change
- Approver Groups for Change Approval Board (CAB)
- Emergency E-CAB and other specialty based Approval groups and Reviewer groups
- Multi-level Approval process supported by Action Option to "Submit for approval", "Withdraw from approval" and possibility of multiple approval levels
- Email Notifications to Approvers / Reviewers with details of proposed change to initiate each Approval cycle upon "Submit for Approval" action
- Manual addition of Approver / Reviewers to a specific ticket which can be enabled or disabled via configurations
- Support of automated decision rules based on Approval Type "All Approvers must approve" and "Any one Approver can approve" to conclude an approval process
- Workflow Automation based on outcome of "Submit for approval" process by specifying next "Action when Approved" and "Action when Rejected"

Configuration Management

Configuration Items

Any component of an IT infrastructure that needs to be managed in order to deliver an IT Service is referred to as Configuration Item (CI). All IT objects like Hardware, Software, Networking Devices, Peripherals, Documentation, etc. are examples of Configuration Items.

Organizations need to maintain up-to-date records of these CIs in an organized way so that historical information about the configuration item, its relationship to other CIs, and other details about its use is available.

Configuration Management deals with providing IT Management a control over the IT Assets such as hardware devices, computer programs, documentation, outsourced services, etc. Configuration Management allows the management to:

- Specify ownership, status, and version related information about a Configuration Item
- Maintain current records about a Configuration Item and a history of changes to the Configuration Item
- Create and maintain relationships between different Configuration Items

Configuration Management enables everyone in Service Management and Service Support to access correct and accurate information about available Configuration Items with their present physical and functional specification.

Configuration Management in Nimsoft Service Desk

The Configuration Management Module in Nimsoft Service Desk provides a structured framework for maintaining an up-to-date record of all CIs of the organization. This module provides a framework to create new Configuration Item Records providing all required information about the Configuration Item and maintaining historical information about a CI.

Nimsoft Service Desk maintains records of Configuration Items belonging to the organization. Configuration Items can be grouped and classified according to their Class, Category, Type, and Item (CCTI).

All essential attributes of a Configuration Item, like its Make, Model, Manufacturing Date, Warranty details, etc., can be stored in the CI record using default attribute templates. Specific attributes of a set of CIs can also be captured using CCTI based Attribute templates.

Categorization (CCTI) can be applied for the Configuration Item, and the CI can be associated with different contacts in different roles like Owner, User, Vendor, Service Provider, etc. One Configuration Item can also be related to other Configuration Items in different domains, and this relationship can be viewed in a CI Relationship graph drawn based on the relationship.

Service Desk Agents can use available CI records and relate CIs to tickets and view information on how CIs are related to each other. Every time a ticket related to a Configuration Item is created, this information is stored in the CI History tab. Self-Service Users can also relate Configuration Items to a ticket by choosing from any CI that is related to them.

Incident Management

ITIL defines an 'Incident' as any event which is not part of the standard operation of the service and which causes or may cause, an interruption or a reduction of the quality of the service. An Incident is an unplanned interruption to an IT service or reduction in the quality of an IT service.

An Incident could be due to a known/existing issue or could be result of a failure or error in the IT object or device. Failure of a Configuration Items that has not yet impacted service is also an incident.

The process of incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, and final closure of the incident are parts of Incident Management Process. An Incidents Ticket can be logged by the Service Desk Agent directly; or it can be created from a Service Request, which actually reports an Incident.

Incidents Management is the process of dealing with Incidents reported to Service Desk by the user or other Service Desk Agents, or automatically detected by Event Monitoring Tools. The focus of Service Desk staff is to provide a solution or at least a work around to the Requester to restore the Affected Service as soon as possible.

The objective of Incident Management is to restore normal operations, with the least possible impact on either the business or the user, at a cost-effective price. After providing a work around, the Incident ticket may be assigned to appropriate support groups who take the ownership for Investigation and Resolution of the issue. The Incident Management Process can be implemented through the Incident Management Module of Nimsoft Service Desk.

Incident Management Life-cycle

An Incident typically passes through four phases. These are:

Phase 1: Logging, Categorizing, Prioritizing, Initial Diagnosis, and Classifying as Major or Minor issue

Phase 2: Searching Knowledgebase for a solution or work around. If required, escalating to higher support level for detailed Investigation. Linking to an existing global issue or creating a child Problem ticket, if required

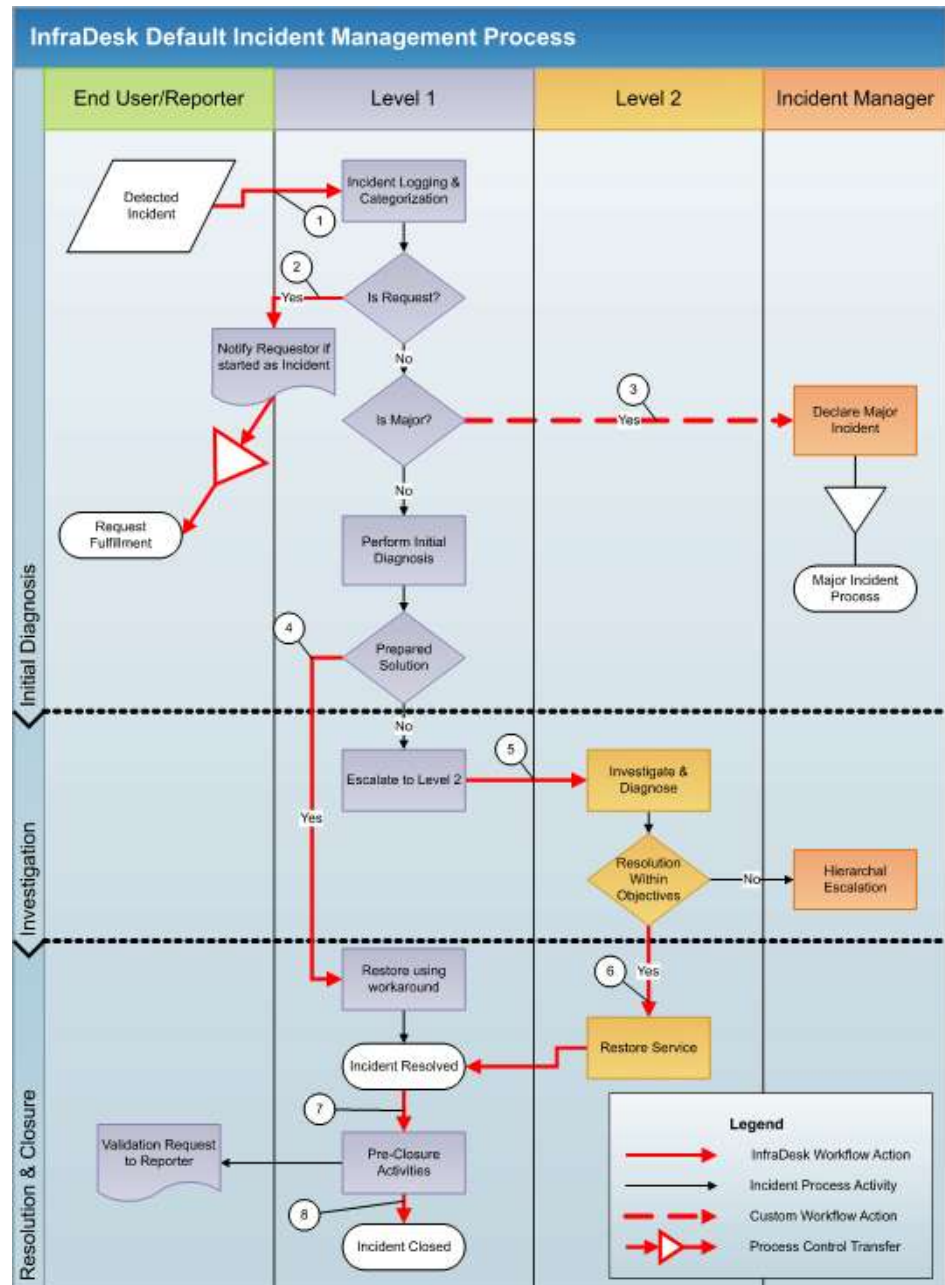
Phase 3: Restoring service as soon as possible using Work Around or solution

Phase 4: Validation of Resolution by User and Closure activities

At each Phase, an appropriate Status and Reason Code will be associated with the ticket. The movement of the ticket through its Life Cycle is determined by the workflow established for achieving the aims of Incident Management.

Incident Management in Nimsoft Service Desk

The Incident Management Module of Nimsoft Service Desk is used to provide Workflow automation using Auto-Route based assignment or Default assignment of Incident Tickets to specific Group(s). It creates a repeatable and measurable Incident Management process within an Organization. It is meant for logging and tracking work on Incident Tickets reported by the Service Desk. The default Nimsoft Service Desk workflow for Incident Management is depicted below.



As application administrator, you can configure an alternate Incident Management workflow depending on the processes and practices followed in your organization. Alternately, you can modify the workflow to be more suitable to the specific needs of your Organization.

Processing of an Incident Ticket typically follows the Workflow design through with the Incident ticket along its life-cycle. The processes could involve simple steps of working to restore the service and resolving the Incidents; or, depending on the severity of the incident, the incident can be marked as Global Issue or related to a Global Issue.

An Incident Ticket could also lead to creation of a Problem Ticket, which could then call for a Change.

Knowledge Management

Service Desk aims to ensure availability of IT Services to the users when they need it. Users may experience issues in using an available service; or may seek assistance or guidance in using a service made available to them. As organizations deal with incidents and problems in an available IT service, they gain experience in responding to user queries and in handling incidents and problems reported by users.

It is important to leverage past experience and other information to provide quick work-around and solutions for Incidents or Problems that Service desk Agents deal with. Knowledge Management provides the ability to store solutions to Incidents or Problem that have occurred previously. It also enables storage and availability of response to user queries and other information needs for users.

Knowledge Management allows users to dig into an available repository of Knowledge Articles in the Solutions Knowledgebase to provide first line of support to the end users. Storing Knowledge Articles to help resolve common and known issues saves the time spent by the Support team in investigating and experimenting with probable resolutions to known issues or issues which have been successfully resolved in the past.

Knowledge Management in Nimsoft Service Desk

The Knowledge Management Module of Nimsoft Service Desk can be configured to create and store Knowledge Base Articles. These articles could be solutions to incidents and problems where symptom, cause, and resolution of the issue can be captured. Articles could also include response to user queries.

Information on Known Outages, Frequently Asked Questions, and other News and Informative Articles can also be captured and published on the Self-Service User Interface via the Knowledge Management Module. Self-Service Users can also be provided access to a subset of easy-to-understand-and-use solutions to routine requests to encourage self-help and to reduce the work load on Service desk.

Knowledge Base Articles can be categorized using the KB Article Category; and the article can be related to available CCTI categorization. When a Knowledge Article is created, Keywords from the article are automatically captured and are used to display matching results during a Keyword search. Key words can also be manually added to the article, if needed.

Service Desk Agents can also be provided permission to Add Solutions from an open ticket to the Knowledgebase. All new articles remain in Draft state. Once reviewed, the status can be set as Approved. If a Knowledge Article is no longer valid or useful, the status can be set to inactive; this makes it unavailable to users.

When Service Desk Agents search for solutions to an open ticket (using the Search Solution action from the ticket), they can access Knowledge Articles related to the ticket. Tickets with matching Keywords and Matching CCTI get displayed. Service Desk Agents can also expand or restrict the search by using the available filters. The solution search can also be expanded to include recently resolved tickets in the search.

Users (both Self-Service Users and Service Desk Agents) can rate an article and view the average rating of the article. Users can also comment on the usefulness of the article and provide feedback comments for an article. This helps manage the Knowledge Base more effectively.

License Type

A Software License is a legal instrument which governs the usage and distribution of software. A software license permits the user to use the software in a way that is agreed upon as per some contractual agreement. A License also controls how a user uses the software.

Nimsoft Service Desk can be accessed by users who have a license to access the product. There are four types of licenses that a user can have for accessing the software. These are:

Self Service User License

This license allows you to access the Self-Service User Interface of the application. A Self-Service User would normally have very limited interaction with the application; and would use features such as logging own requests, viewing status of requests logged, searching for information stored within the application, and viewing information that has been published for them.

Floater License

This license allows users to access the normal Agent/Administrator interface of the application. A user with a floater license can access the full suite of features available in the application.

The features and functionality that a user assigned with a floater license accesses is, however, controlled by Permissions managed by the Application Administrator.

A floater license is not tied down to one specific user. It is applied as a concurrent user license. Typically, there would be more number of users than the number of floater licenses purchased. A floater license allows a fixed number of users to log on to the application at any given time. Only as many users can access the application at a time as the number of floater licenses.

Self-Service Licenses are also like Floater Licenses as it allows as many users to access the application at a time as the number of floater licenses. However, unlike with Self-Service License, users with floater license get access to the main application interface.

Fixed License

A Fixed license allows only an identified user to access the application at a time. A contact assigned a fixed license can access the application at any time. Fixed licenses are ideal for users who would need access to the application at all times.

Web-Services License

Web-Services license is used by organizations that want to create a web-services client to interact with Nimsoft Service Desk. The web-services client can be used to invoke supported functions in the application.

Problem Management

A Problem is the "Unknown Cause" of one or more Incidents. It is often identified as a result of multiple smaller Incidents. A Problem is usually reported when an Incident is so severe that a Configuration Item could fail or when Service Availability could be severely affected.

While Incident Management deals with quick restoration of service by applying a quick solution or work-around, Problem Management deals with determining and eliminating the Root-Cause in such a way as to prevent reoccurrence. Usually Problem Tickets are logged before a critical failure - to identify the root-cause of the incidents and prevent a failure. Problem Tickets can also be logged to review a failure and to take corrective action.

The objective of Problem Management is to minimize the adverse impacts of Incidents or Problems caused by errors in the IT infrastructure, and to initiate actions to prevent recurrence of Incidents related to those errors.

The primary objective of Problem Management is to find the Root Cause(s) or the Incidents which led to creation of the problem and resolve the Root Cause so that current incidents and their future recurrence is eliminated or at least the impact is minimized if incidents cannot be totally prevented.

Problem Ticket processing also involves investigation and diagnosis which is similar to the incident management process. However, the focus is entirely on identifying the root cause of incidents impacting the business. Problem tickets deal with issues of more generic and global level compared to Incident tickets but the actions and activities related to them are very similar.

Problem Ticket Life Cycle

A Problem typically passes through four phases which involve:

Phase 1: Reactive and Proactive Problem Detection, Categorizing, Prioritizing.

Phase 2: Detailed Investigation, Diagnosis of Root cause, offering Work Around

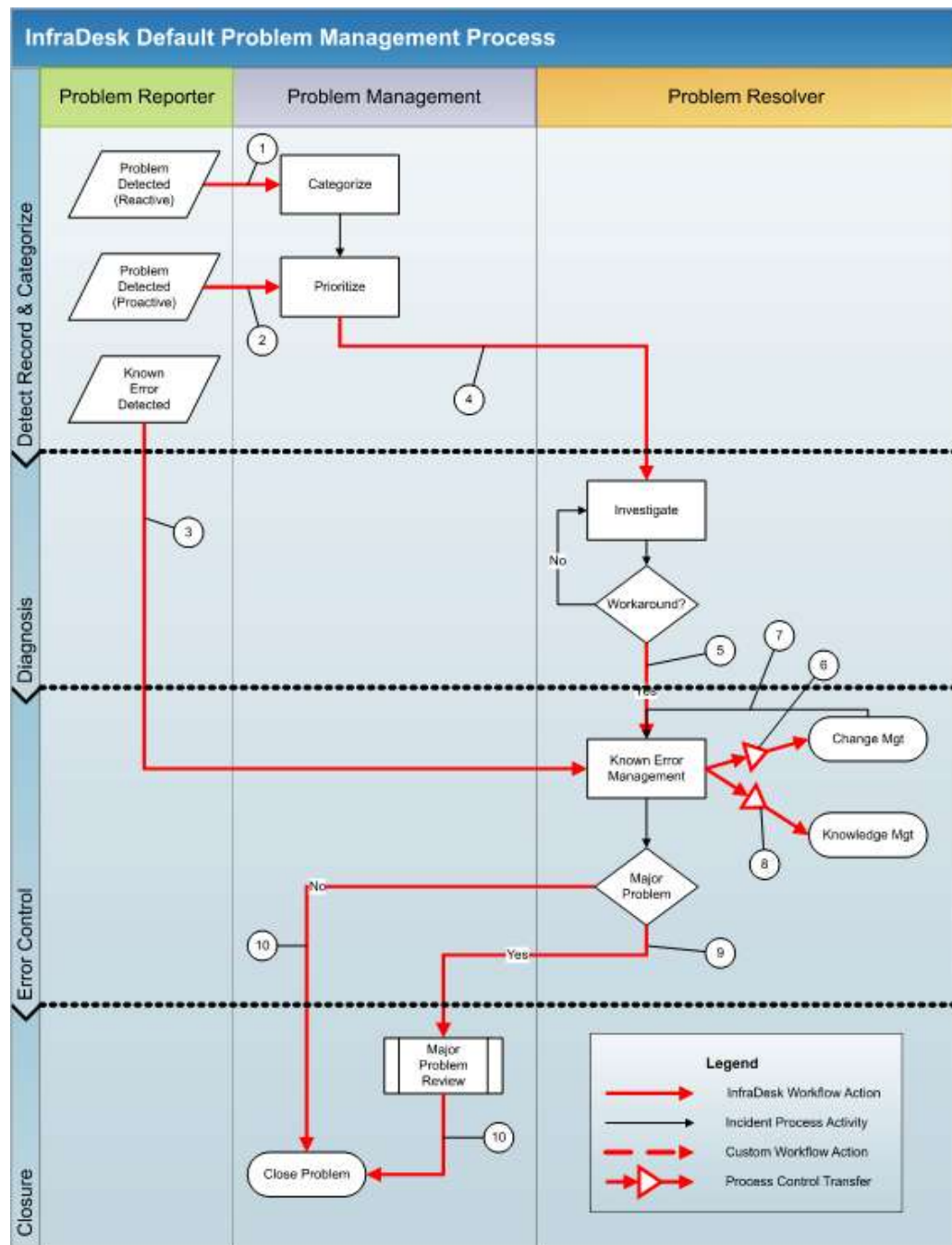
Phase 3: Managing Known Error, Root Cause removal through Change Management

Phase 4: Closure Activities including Review for Major Problems

Problem Management in Nimsoft Service Desk

The Problem Management Module of Nimsoft Service Desk is used to provide workflow automation using Auto-Route based assignment or Default assignment of Problem Tickets to specific Group(s). It creates a repeatable and measurable Problem Management process within an organization. It is meant for logging and tracking work on Problem Tickets reported to the Service Desk.

The default Nimsoft Service Desk Workflow for Problem Management is depicted below.



As application administrator, you may configure an alternate workflow or modify the workflow to make it more suitable to the needs of your organization.

Processing of a Problem Ticket follows the workflow. Problem Ticket moves along its life-cycle depending on the actions taken on the ticket at different stages in the workflow. The processes involve the various phases on Problem Management to identify a root-cause of the Problem and find ways to solve root-cause.

If the severity of the Problem is high, it can be marked as Global Problem, and other Incident or Problem Tickets or other Service Request tickets could also be related to it.

A Problem Ticket can be created off an Incident Ticket; and a Problem Ticket could lead to the need for creation of a Change Ticket to resolve the Problem.

Request Management

A request from a user for information or advice regarding the use of an IT service, a request for a standard change, or access to an IT service is called Service Request. A Service Request may also report an issue faced by the user.

A Service Request is generally the starting point for all interactions between the users of IT Support and the Service Desk.

In some organizations, all requests that are logged and handled by the service desk are logged as Service Requests. An agent working on the request may later want to create an Incident ticket or a Problem ticket or a Change request against the Service Request, if required, and work towards closure of the Request.

Request Management is the process of managing a Service Request through its life-cycle from submission of the request through to delivery of required information or execution of standard change or providing a work around / solution or escalating the Request for further processing as an Incident.

The work-flow or process that enable these Service Requests to be appropriately submitted, routed, approved, monitored, and delivered form a part of Request Management.

- Request Management involves establishing a Request Fulfillment Process with aims to:
- Provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services (e.g. licenses and software media)
- Assist with general information, complaints, or comments

Service Request Life Cycle

A Service Request typically passes through three phases which involve:

Phase 1: Logging, Capturing information, Validating

Phase 2: Fulfillment activities or escalation activities

Phase 3: Closure activities

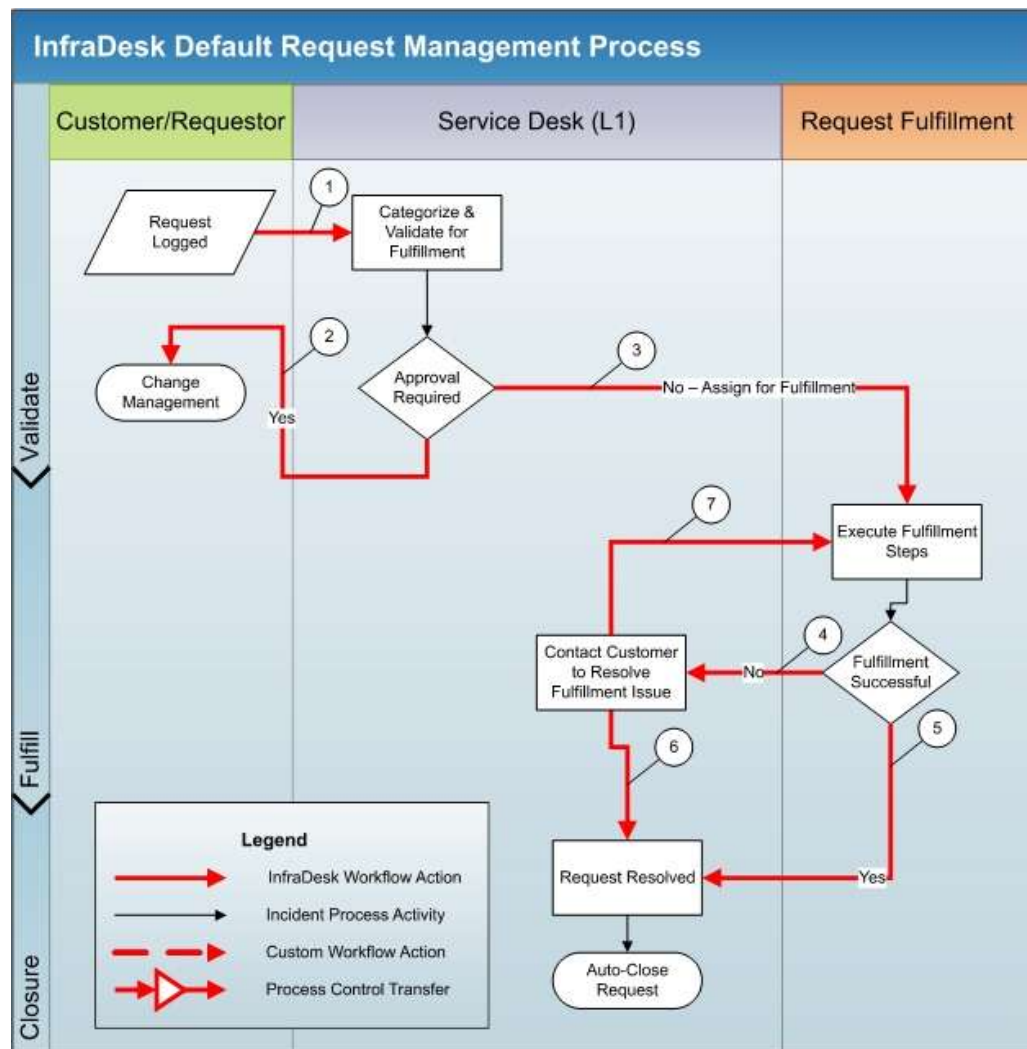
At each Phase, an appropriate Status and Reason Code will be associated with the ticket. The movement of the ticket through its life-cycle is determined by the workflows established for achieving the aims of Request Fulfillment.

Request Management in Nimsoft Service Desk

Request Management Module of Nimsoft Service Desk is a tool to provide workflow automation using Auto-Route based assignment or Default assignment to an Assigned Group. It creates a repeatable and measurable Request Fulfillment process within an organization. It is meant for logging and tracking work on Service Request received by Service Desk.

Processing of a Service Request may typically involve workflows depicted in Request Handling Process. These may involve simply fulfilling a standard pre-approved template based Request and closing it or searching the solutions knowledge base to provide a temporary work around to an issue and then escalating it as an Incidents ticket or linking to an existing Problem, which may later lead to a Change Request.

The process and progress on Service Requests can be managed using the Request Management Nimsoft Service Desk Application. The default workflow for Service Request available in Nimsoft Service Desk is demonstrated below.



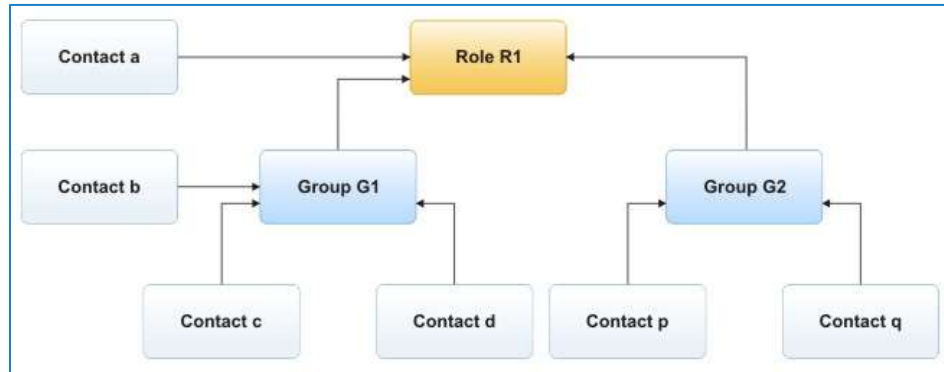
As application administrator, you can configure an alternate workflow or modify to be more suitable to the specific needs of the organization.

All tickets logged by the Self-Service Users, without using a Ticket Template, get logged as Service Request. Similarly; all ticket logged via email (without a pre-defined Subject) sent to the Support ID get logged as Service Request. An Agent (usually offering L1 Support) reviews the request and moves it along in its life cycle.

Roles

A Role indicates the actions and activities assigned to, required of, or expected of a person or group. A role can define a person's tasks, responsibilities, qualifications, or expectations. It may be associated with a collection of software privileges or permissions.

You can create roles such as Change Manager, Service Delivery Manager, Service Desk Supervisor, CAB Member, Reporting Managers, etc. A contact or a Support Group can be linked to a Role; and you can assign permissions to a role.



All permissions granted to a Role are inherited automatically by the Contacts and by all members of Support Groups who are associated to the role. This is an effective way of managing permissions to Defined Searches, Reports, Templates, and all other aspects of Nimsoft Service Desk, where permissions are managed.

Roles can also be used to manage the sending of communication templates to stakeholders. The Send to, Cc, or Bcc field in a Communication Template can be populated with a Role so that the communication will be transmitted to all members of the Role.

Service Desk Tickets

A ticket is a transaction document that records all the information related to a request. This includes details of a User Request, Incident, Change Request, or a Task/Work Order.

Tickets have different fields and tabs where specific information related to the request can be recorded and stored. A Ticket also carries records of the efforts undertaken to diagnose and resolve the problem and steps taken towards fulfilling the request.

A ticket forms the basic entity in Trouble Ticketing, Issue Tracking, and Service Desk Applications like Nimsoft Service Desk. All requests logged by an end-user are logged as a ticket in Nimsoft Service Desk.

Self-Service Users can log a ticket by sending an email to the support desk ID configured for the slice. The email gets logged as a ticket in the application. Self-Service Users can also log a ticket directly from the Self-Service User Interface. The ticket gets assigned to a support group as per an auto-route or default routing.

Service Desk Agents work on tickets logged by Self-Service Users. They can also log a ticket on behalf of the Self-Service User, especially if the request is submitted via phone. Service Desk Agents can also log tickets for other requests for support related to the IT Services and IT Infrastructure.

A ticket carries all information related to the transactions on the ticket including manual and automatic actions and communications.

Service Feedback

Service Feedback includes documents that are used to solicit feedback from customers/users/user groups regarding their satisfaction level with identified parameters of a service.

This qualitative information regarding the customer's perception of the quality of service on given parameters gives the service provider a view of what the users think about the services provided. Identifying the trends in satisfaction levels allows the service provider to develop action plans for continuous improvement.

Nimsoft Service Desk Application Administrator can set up a Service Feedback Form based on the type of feedback they would like to solicit from the end users of support. Further, the Administrator can schedule a Feedback Form to be sent out automatically either at a fixed duration or after a fixed number of requests.

A Schedule can also define a survey as "Anonymous" so that Respondent's identity is not required and frank feedback can be given. Respondents can also be allowed to submit their feedback more than once if the schedule is anonymous. A survey, as part of a schedule, can be sent to Contacts, Groups, or Organizations.

Administrator can manage participation of users in the service feedback process by enabling or disabling service feedback for an Individual Contact, all users related to a Support Group, or an Organization.

A schedule once set, gets initiated and ends as per the dates or parameter set. If required, the schedule can be aborted before completion.

Administrator (or any designated contact) can access reports related to Service Feedback Schedule to draw conclusions based on the survey response.

Service Level Agreement

Service Level Agreement (SLA) is an agreement between an IT Service Provider and a Customer that describes the IT Service and the performance expected. In ITSM Service Level Agreements are used to define aspects related to the availability of the IT Service, service conditions, etc.

When applied to Support of IT Service, the time taken to respond and time taken to resolve User's Requests forms the basic measure of actual Service Level against an agreed performance target. SLA can be taken to refer to the contracted delivery time for a service or performance.

Service Level Agreements lay out the contracted agreements in terms of delivery time of a service or time established for restoration of service.

A Service Level Agreement is usually between the customer (end-user of IT support) and the service provider. Within the organization of the service provider, there can be internal agreements for ensuring that services are delivered within the SLA. These agreements are called Operational Level Agreements (OLAs). Service delivery can also be measured against some agreed upon contracts called Under Pinning Contracts.

Service Level Management

IT Organizations are increasingly looking at ways of quantifying and measuring the level of service and support provided to the end users. One way of imposing quantitative measurements is by establishing Service Level Agreements.

Service Level Management deals with the process of negotiating Service Level Agreements and of ensuring that these are met. Service Level Management is responsible for ensuring that all IT Service Management processes, Operational Level Agreements, and Underpinning contracts are appropriate for the agreed Service Level Targets. Service Level Management monitors and reports on Service Targets.

Regular reviews related to services and actual performance and agreed upon service level targets, with the customer are desirable for continuous improvements.

Nimsoft Service Desk allows users to apply Service Level Management on ticket by setting up measurements against pre-defined Service Metrics.

The Key units to measure SLA Performance are Service Metrics and Service Targets.

Service Metrics

Service Metric defines what is to be measured. This can be a measurement such as Ticket Response time (i.e. the time taken for a ticket to move from New Status to Active Status), Ticket resolution time (time taken for the ticket to move from Active Status to Resolved Status), etc.

When several groups are involved in working on a ticket one after another, the performances of individual groups can be monitored in terms of Group Response Time and Group Ticket Holding Time. Nimsoft Service Desk provides a set of pre-defined metrics which can be applied to measure SLA Compliance of a ticket.

Service Target

Service Target defines the time allocated for completing the activity being monitored against a service level metric. For example, based on the Service Level Agreements, Ticket Response Time could be set as 15 minutes. The time allotted is called the Threshold value. While monitoring the Service Target, the Nimsoft Service Desk Administrator can set Violation and Non-violation thresholds and define action to be taken on threshold violation.

As Application administrator, you can configure SLA Targets and threshold rules suited to your business needs. You can also configure Email and Phone notifications to be sent out when a target threshold is approaching. Service Desk Agents\Analysts or the Support Group working on the ticket can take action in response to the notification to ensure that the ticket is acted upon within defined target thresholds.

SLA measurements are also governed by factors like Support Group Business hours (the time that the service group is available to work on requests) and Service Availability (what is the time a service is agreed to be made available).

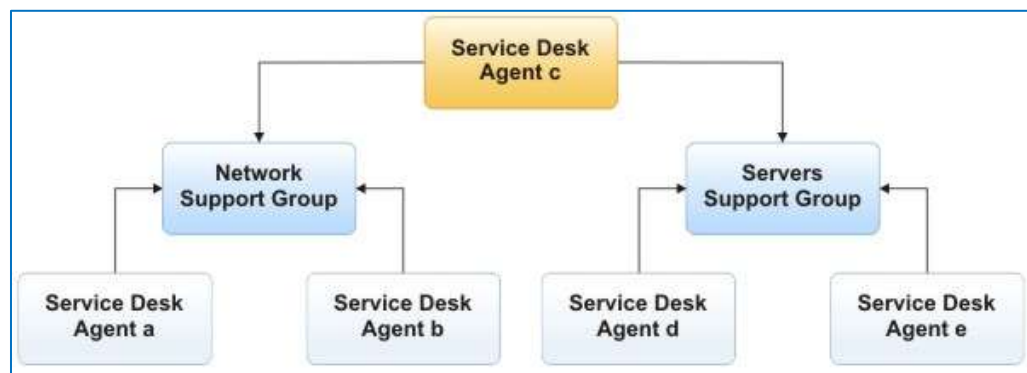
Nimsoft Service Desk allows for the ability to pause SLA calculations, if required. While configuring a Service Target you can choose tickets in certain status/es and enable the Measured Time calculation for these tickets to be paused. Thus when a Service Target is applied to a ticket, the measured time calculation excludes the time spent by the ticket in the "Paused" status. The Due Date field is displayed as "To be determined".

Note: For enabling SLA Phone Notifications, you will need to buy a license from MIR3. Phone Notification is an external service provided by MIR3, and not a default feature available with Nimsoft Service Desk. Currently Phone Notifications are supported only for SLA Notifications, and not other notifications sent out by the application.

Support Groups

Support Groups refers to the grouping contacts for the purpose of providing support on similar tasks. Grouping contacts who are capable of handling a given tasks ensures responsibility taken by a number of people instead of an individual. This reduces dependency on any one individual to work on a issue. Anyone from the group can take ownership of the issue and start working on it.

A contact can be part of multiple support groups; and if so related, the contact can view tickets assigned to all Groups that the contact is part of. Also, permissions can be assigned to a Support Group rather than to individual contacts. The contact inherits permissions from all support groups that the contact is related to.



Grouping contacts into support groups allows configuration of auto-routes on tickets. It ensures that at least one member of the group will be available to handle a request at a given time. Support Groups ensure that a request is not waiting in the queue of an individual when the person is not available to work on the request.

Contacts can be member of more than one support group, and access options applicable to all groups that they are associated with. However, only one of these groups will be designated as the primary group of the contact.

Support Groups can also be earmarked for the different purposes, by specifying what the support group will be Used For. A Support Group which is meant to be used for Approvals can be marked as Used for Approvals. All support groups that are marked as Used for Approvals will be displayed when taking an action of configuring Approval Groups and when choosing approvers or reviewers for a ticket.

Time Zones

In globalized economies, IT service management may involve Service Users and Service Support Groups situated around the world in different countries and varying time zones. Operating on 24X7 basis means that the time stamps for transactions must be recorded on a standard basis such as GMT or Universal Time. Moreover availability schedules of IT services need to be specified with reference to a time standard.

A user, however, can understand and utilize the time related information much more easily if his/ her view of time information is expressed as per his/ her time zone. Nimsoft Service Desk therefore, takes into account the time zone of the logged-in user and performs the necessary time conversions to user's time zone for displaying time related information.

In Nimsoft Service Desk, the concept of Time-Zone is used to enable a logged in user to view transactions and details in relation to his/her physical time. Time-Zone can also be associated with Support Groups to indicate availability of a support group.

A Time-Zone, Calendar period of applicability, Work week pattern, and Holiday List are taken into account when calculating availability of a support group or service and in setting auto-routes.

Time-Zone related calculations are applied to tickets particularly for calculating SLA Compliance in terms of Response Time (Time taken by an assigned individual/group to accept assignment and take ownership of a ticket) and Resolution Time (Time taken by an assigned individual/group to resolve the ticket).

Time Zones are also useful in calculating Service Hours, which is the agreed time period when a particular IT Service should be Available. For example, Availability Schedule of a CI defined as Service could be "Monday-Friday 08:00 to 17:00 except public holidays".

Time associated with an auto-route enables effective auto-routing of tickets based on support group availability. Multiple auto-routes can be configured for a similar type of request based on availability at different times.

Single Sign On

Single Sign-On is a property related to access control of multiple related but independent software application. Once a user logs into a system with this property; the user gains access to multiple systems without having to enter user credentials individually in each system or application. A reverse property; Single Sign-Off, terminates access to multiple systems with one single action of signing off.

Nimsoft Service Desk Single Sign On tool supports SAML 2.0 based authentication standards for authenticating Nimsoft Service Desk users with an identity provider.

By using the simple application interface (under Manage Configuration link in the Application Setup Module); the Application Administrators can configure the administrative components needed to enable Single Sign-On (SSO) as well as authenticate users in Nimsoft Service Desk.

Once Single Sign On is configured; users can seamlessly log into Nimsoft Service Desk without being prompted for application user name and password.

Ticket Related Concepts

Action Options

Action Options are actions pre-defined by the administrator, which guide the Service Desk Agents and Support Groups to follow the workflow while processing the tickets. An Action Option is customizable to the specific ticket form and gets applied to the ticket when the ticket matches conditions on the Action Option.

Taking an action on the ticket using the action option, results in the ticket conditions getting changed. Fields like Status, Reason Code, Assigned to, CCTI, etc., get updated as per pre-defined configurations. A template based communication can also be set off by taking an action on the ticket using an Action Option.

Action Options are available in the Take an Action button on the ticket. The Action Options available for a ticket at a particular stage of the ticket life-cycle are controlled by the workflow actions configured for the ticket.

For example, consider a Service Request where the Status is 'New' and Reason Code is 'None'. The Take an Action option on the ticket could display Action Options like:

- Accept Assignment
- Take Ownership
- Assign to Group
- Request to Delete Ticket

If the Agent chooses the Action Option of Take Ownership, then, based on the workflow configurations, the Ticket Status could change to 'Active' and the Reason Code would change to 'In Progress'. The Assigned to Individual field would display the name of the Service Desk Agent who has taken ownership of the ticket. An email notification could get sent to the ticket requester about the change in status of the ticket.

At this stage, if the Agent working on the ticket wants to move the ticket further along the life-cycle, the Action Options available could be:

- Re-assign within Group
- Escalate to Group
- Pending Additional Information
- Resolved

Such movement of tickets from one state to another is controlled by Action Options. Action Options are configured by the Application Administrator depending on the type of workflow they wish to establish for a request.

They are a way of ensuring that the workflow for a given ticket type is followed by the Service Desk Agent or Support Group when working on the ticket.

Workflow actions can also be triggered by Auto-routes, which can be set off by some Matching Conditions. For example, if a ticket is a Standard Change Request for Creation of new User Accounts, the request can be automatically assigned for approval via an auto-route.

Auto-Routes

Requests for support coming in from the end-users, need to be assigned to specific support group or individual based on the nature of the request or issue for appropriate action towards its resolution.

If all tickets are processed through the default assignment group specified in the Slice Configuration, and the default group then takes on the task of sorting through the request and assigning it to an appropriate group, it can add to the total time taken to resolve a ticket.

Auto-Routes are configured to automate the process of assigning a ticket to specific group based on specific criteria. By setting up auto-routes, new tickets can get assigned to a specific individual or support group based on matching conditions specified on the auto-route.

Auto-Routes get applied to a ticket based on a set of pre-defined rules and values on various parameters of a ticket. Auto-routes can be designed based on availability of resources at a location at a given time, priority of the ticket, CCTI, etc. Auto-Routes can be applied to tickets logged directly in the application by the user (Service Desk Agents and Self-Service Users) and by tickets created via emails to Support mail ID.

Case ID for Tickets

Case ID enables maintenance of relationship between dependent or associated tickets. This is useful where several tasks need to be completed for request fulfillment and therefore Child Tickets are created from an open Parent Ticket.

For example, an HR Request for providing IT Systems for a new employee could include tasks like provisioning a desktop machine, configuring email for the new employee, providing access rights where needed, etc. Thus a Parent Request would have Child Tasks for each of these individual tasks and all of them can be identified using the Case ID.

Case ID is also useful when one type of ticket leads to the creation of another type of ticket (say an Incident or Problem ticket calls for a Change, and hence a Change ticket is created out of the Incident). In such cases too, the Case ID enables easy referencing of all the activities resulting from one request. The subsequent ticket is created as a child ticket.

When a Child Ticket is created, it inherits the Case ID of the parent ticket; and a new Ticket ID gets further assigned to it. For example, if a ticket has an ID 398-23 and a child ticket is created from this request, it may have a Ticket Number based on case ID such as 398-42 where 42 is the ticket number for the child ticket.

Service Desk Agents working on the ticket can manually move the Case ID to a desired Case Number, if required, and if so permitted by an administrator.

The Case ID functionality is not imposed on all users. You can choose not to use the concept of Case ID by modifying the slice parameter accordingly. In case Case ID is not used, a constant Case # will be generated for tickets based on ticket type.

Categorization of Tickets

Categorization is the process of logically grouping objects and entities for a specific purpose. Categorization provides a means of recognizing objects, differentiating them, and understanding them via similarities and differences in the context of their use.

Tickets logged in Nimsoft Service Desk can be categorized for more effective management of the ticket through its life-cycle.

Categorization of tickets facilitates effective auto-routing of the tickets to the appropriate group. For example, the Administrator can set up an auto-route that if a ticket has the Class as Printers and Category as Laser, it should be auto assigned to a specified support group.

Tickets with a specified Categorization bypass the default assignment group and can be worked upon directly by members of a specialized group. This reduces time involved in the ticket getting assigned to different groups and reduces unnecessary transactions between multiple groups.

Categorization of tickets also enhances solution search executed from an open ticket. The solution search will display solutions with the same categorization as the ticket; and if enabled, tickets with the same categorization will also be displayed in the Search Solution action.

Service Desk Agents working on the ticket can categorize a ticket as appropriate to the nature of the request. Self-Service Users can categorize request by "Type". This Categorization facilitates assignment to the appropriate team.

Global Issue

ITIL processes recommend a well-defined process starting with Service Request through Incident Management, Problem Management, and Change Management using appropriate Service Desk tickets.

When a specific error results in logging of several Service Requests, it leads to an Incident; or when several Incidents arise due a common root cause, it leads to recognition of a Problem. These tickets are related and need to be linked.

An Incident or a Problem is designated as a Global issue when it represents a group of similar Service Requests or Incidents. When the Global issue is addressed and resolved the other tickets also get addressed.

When a Global ticket is resolved or closed, the status and reason codes for tickets related to it are also updated. The solution applied to the Global Ticket is also applied and associated with the related tickets.

Resolution of the Global Issue, however, does not result in resolution of open task tickets of a Related Ticket (Incident or Problem related to the Global Issue).

To avoid this and to ensure that related Parent tickets are not resolved or closed when the child Task Tickets are open, you can choose the Special Function of 'Check for Open Tasks' when configuring a workflow action for Incident or Problem tickets.

If the workflow action Special Function is set to Check for Open Tasks, the parent ticket will not be resolved or closed automatically when the global issue is resolved.

- Cause and Resolution details will get updated on the parent ticket
- Set field values from the global ticket will not get applied to the parent ticket
- The parent ticket will not be resolved/closed
- A communication will be sent to the parent ticket owner to resolve child tickets and close parent ticket

If the special function is not set to Check for Open Tasks:

- Cause and Resolution details get updated on the parent ticket
- Set field values from the global ticket will get applied to the parent ticket
- The Parent ticket will be resolved/closed
- A communication will be sent to the parent ticket owner about the action on the parent ticket.

Prioritization

Prioritization is the process of determining which task or activity takes precedence when several issues are to be worked upon at the same time. The fields that allow prioritization of a ticket are Priority, Impact, Urgency, and Severity.

When a Self-Service User submits a request using the Self-Service User Interface, he/she can set the priority and/or urgency of the request depending on how quickly the ticket is to be addressed; or how critical the issue is.

Request logged using a Request Template can also have pre-defined values in the Priority field. The ability of Self-Service Users to view and update prioritization on a ticket can be hidden by the application administrator by modifying the relevant Configuration Parameter.

Service Desk Agents/Analysts can set Priority of a ticket being logged based on its Urgency and Severity. If an issue is impacting several users, or if it is impacting a large number of services or a business critical service, its severity can be said to be high. Similarly, if an issue needs immediate resolution, then the urgency can be set as high. An issue with high urgency and high severity can be set as High Priority.

Prioritization allows the Service Desk Agent to decide that the Request / Ticket needs immediate attention and can help the agent move its resolution ahead of other open requests. Values in the Prioritization fields can also trigger an auto-route to get applied to the ticket; or determine the workflow actions that get applied to the ticket.

Guidelines regarding how to determine the Priority based on values assigned to Urgency and Severity of an issue is specific to each organization. The values provided in standard drop down (None, Critical, High, Medium, and Low) can be customized for an organization by Administrator using the “Manage Value Lists” functionality in Workflow Tools.

Priority of a ticket can also be used by in defining matching conditions for Action Options, Auto routes, and Service Level Targets so as to better manage tickets that have been defined as High Priority.

Task Groups & Task Flows

Task tickets are created as Child Tickets from a Parent Service Request, Incident or Problem Ticket or a Change Ticket. All activities that are needed to be performed towards completion of a parent request can be identified, task tickets can be created, and the task tickets can be assigned to different stakeholders for execution.

Service Desk often receives standard or repetitive request, such as, Provisioning of IT Systems for a new employee, De-provisioning of IT systems of an outgoing employee, Upgrade of Hardware or software, etc.

While it is not possible to predict exactly when these requests will be logged, it is possible to identify the set of tasks that need to be done towards resolution of these requests.

For such repetitive tasks, Task Templates can be configured. For standard sets of tasks, Task Groups and Task Flows can also be configured.

Task Group

Often, several tasks need to be performed towards one unit of work or activity. For example, provisioning of a new user would involve creating user accounts for several internal or external applications. Ideally, there would be one task template created for provisioning of the user account for each application.

Task Groups can be configured to group together all task templates for a related set of activities. Task Groups can be used to ensure that individual components within one activity are identified and logged as a separate ticket, and yet, they remain part of a larger unit of work. For example, you can configure a Task Group for User Account Creation and all task templates for user account provisioning can be grouped together in this Task Group.

Tasks in the task group can be assigned to different individuals or support group or to the same individual or support group, as appropriate.

Task Flow

For execution of some standard requests logged with support, Service Desk would undertake a series of activities - usually in a pre-defined sequence. A Task Flow can be configured for such requests, where pre-determined sets of activities need to be executed in a systematic order for successful completion of the request.

For example, fulfillment of a request for Provisioning of IT Systems for a new recruit would call for several activities like:

- Identification of systems and software requirements
- Obtaining approvals for system provisioning
- System provisioning (hardware, software, networking, etc.)
- Provisioning of user accounts into various internal and external applications
- Testing the system for access, performance, etc.

Successful closure of all these activities would lead to successful resolution of the parent request for user provisioning.

A Task Flow can be configured using a combination of independent Task Ticket Template and Task Groups. A Task Ticket or Task Group can be assigned a Sort Order, which determines the sequence in which the task ticket is created.

When Status of a preceding Task Ticket or Task Group is set to Resolved or Closed, the next Task Ticket or Task Group is created and assigned as per the assignment rules configured.

Automated workflow actions can also be configured on Task Flows where you can define Action on Success of a Task Ticket or Task Group and Action on Failure of the Task Ticket or Task Group.

Based on Success or Failure of the Task Ticket, the pre-defined action will be executed on the Parent Ticket. If a Task Flow was unsuccessful, you can correct the issue which caused the failure and resubmit the Task Flow.

Configuring Task Flows allows effective management of several activities that contribute towards resolution of a request.

Task Management

Resolution of a request logged with the Service Desk could often involve performance of several related activities, which together enable fulfillment of the request. For managing these related activities, Task Tickets can be created.

For example, consider a request for upgrade of hardware being used by a group of users. This would typically call for a Change Ticket to be logged. For Execution of this request, there would be several tasks that need to be performed, like identifying hardware components to be upgraded and possible alternatives, procuring quotations for cost of upgrade, compiling cost report, submitting the request for approval, etc.

Based on approval decision, further activities will need to be done towards procuring the required hardware, upgrading the hardware, and testing performance. Only when all these activities or tasks are completed appropriately, the request can be fulfilled.

Task tickets are created as Child Tickets from a Parent Service Request, Incident, Problem, or a Change Ticket. All activities that are needed to be performed towards completion of a parent request can be identified and task tickets can be created; the task tickets can then be assigned to different stakeholders for execution.

Task Tickets can be assigned to different individuals or groups who are to carry out the actual task; and the owner of the Parent Ticket can continue owning the main ticket and ensure that all tasks are completed before resolving or otherwise closing the parent ticket. Tasks need to be carried out in a given sequence specified as Task Order.

For repetitive tasks, Templates for single tasks can be created by the Administrator. Where a group of tasks need to be done to fulfill a standard request, the Administrator can set up a Task Group template using templates of single Tasks. Further, Task flow template can be created using both Task groups and single Tasks. For each task within a Task group or a Task flow, an individual Task ticket is created.

The Administrator can configure workflows for the tasks to be assigned to a specific individual or group depending on the task template selected. For tasks that need to be assigned to specific people, auto-routes can be set up; and for tasks that need to be carried out in a specific sequence, specified Task Order can be defined.

To execute a Task Flow, all its Task tickets are NOT created at once. Only on completion (status=Closed) of all tasks of a group, the Task tickets for next are created. For Task Flow templates only, automatic “Action on successful completion” and “Action on failure” can be configured by your Administrator for each task.

Task Ticket Life-Cycle

As Task Tickets are not created as independent entities, they generally follow the life-cycle of the parent ticket from which they are created. The basic stages of a Task Ticket are:

- Creation
- Assignment
- Execution
- Closure

Some aspects unique to Task Tickets are:

- Task Tickets can be created only as Child Tickets to Service Request, Incidents, Problem or Change Tickets. You cannot create independent Task Tickets.
- For repetitive Tasks, templates for single tasks can be created by the Administrator.
- Task Group template can be created using templates of single Tasks.
- Task Flow template can be created using both Task Group and single Tasks.
- For Task Flow templates only, automatic “Action on successful completion” and “Action on failure” can be configured by the Administrator for each member task.

Task Management in Nimsoft Service Desk

Nimsoft Service Desk extends Task Tickets as an additional module to enable smooth execution of tasks necessary to offer an IT Service supported by the Service Desk.

The advantage of using Task Tickets is that the ownership of the parent ticket can remain with one Agent who is responsible for it, while individual units of work are carried out by resources who are assigned the Task tickets. They close the Task tickets as and when work is completed. Using an administrator configured Workflow Actions, Agents can check if all child tasks have been closed or not, while closing a Parent ticket.

Task templates, Task group templates, Task Flow templates, Auto routes, and Workflow Actions can be configured for Task tickets. Task Ticket templates can be associated with Auto Assign action and task tickets can be set to be auto created based on workflow actions. The Application Administrator can manage these configurations to effectively manage task tickets.

Ticket Assignment

A ticket that is created needs to be acted upon by an individual or group so that required action can be taken towards issue resolution or request fulfillment. This act of moving a request to the individual or group that is required to work upon it is called Ticket Assignment.

Unless a ticket is assigned to a Service Desk Agent or a Support Group which a Service Desk Agent is part of, the Agent will be unaware of the existence of the ticket and will thereby be unable to work on the request submitted.

Ticket Assignment can be done manually by a Service Desk Agent or it can be automatically assigned to a specific support group or individual based on either auto-routes or based on default assignment setting managed by the application administrator.

When a Self-Service User logs a ticket via email, depending on the Subject of the mail, an auto-route can get associated with the ticket; and the ticket can get auto-assigned to a specific group.

However, if no such matching condition exists, the ticket gets assigned to a default Support Group as configured by the application administrator. This Support Group then modifies the ticket and manually assigns the ticket to an appropriate Support Group or Individual.

Based on availability of Resource, expertise, specialization, etc., a ticket can be assigned to a specific individual or to a support group; and any member of the group can accept the assignment and act upon it. Reassignment can be used to escalate to a group / individual at higher level if nature and priority of a Ticket requires it.

Service Desk Agents who work on the ticket can accept assignment of the ticket, reassign the ticket to another support individual or support group, escalate and assign the ticket to a higher group, and perform other such assignment related actions that are available on the ticket in the Take an Action Option.

Accepting assignment or ownership of the ticket is usually the first step in working towards closure of a ticket.

Ticket Custom Fields

The various fields in a form provide a structured way of capturing information essential towards resolution of a request. All ticket forms in Nimsoft Service Desk capture the essential information needed for that type of ticket. These fields are called Standard Ticket Fields.

However, as per the customer's individual need or depending on the specific requirements of a given request, there could be a need to seek additional information required to service the request.

For example, when creating a Ticket for Training Requests for employees for using particular software, it may be considered important to include like Employee Name, Employee Code, and Availability Time. Such details are not part of the standard ticket form.

To facilitate building of such fields, which are unique to each organization's context and specific to ticket types, Nimsoft Service Desk allows you to create Custom Fields on a standard ticket form.

A Custom Field can have its own field value type like Text, Number, Date/Time, Check boxes, List, and Radio Buttons. You can also have predefined acceptable values for these fields.

Custom fields are displayed in the Additional Information Section of the ticket on the Self-Service User Interface, and the Additional Information tab on the Agent Interface.

While configuring a custom field template, the administrator can specify whether it should appear on the Self-Service User Interface or not. In this way, the administrator can control visibility of Custom fields to Self-Service Users.

Related Custom fields can be grouped together under a Section Header, to appear more systematic and organized. Different types of Section Headers can be configured to meet different grouping needs.

Custom Fields can be included in ticket templates for specific types of tickets; where like all standard fields, field values can be set and a field can be labeled as Required field. Custom Fields can also be used to set up auto-routes and manage the workflow actions on the tickets.

Data on the Custom fields can also be made part of the pre-defined searches and can be extracted into the reports drawn using the reporting engine. Tickets, when printed, also show the details included in the custom fields, grouped into sections under a section header, if configured.

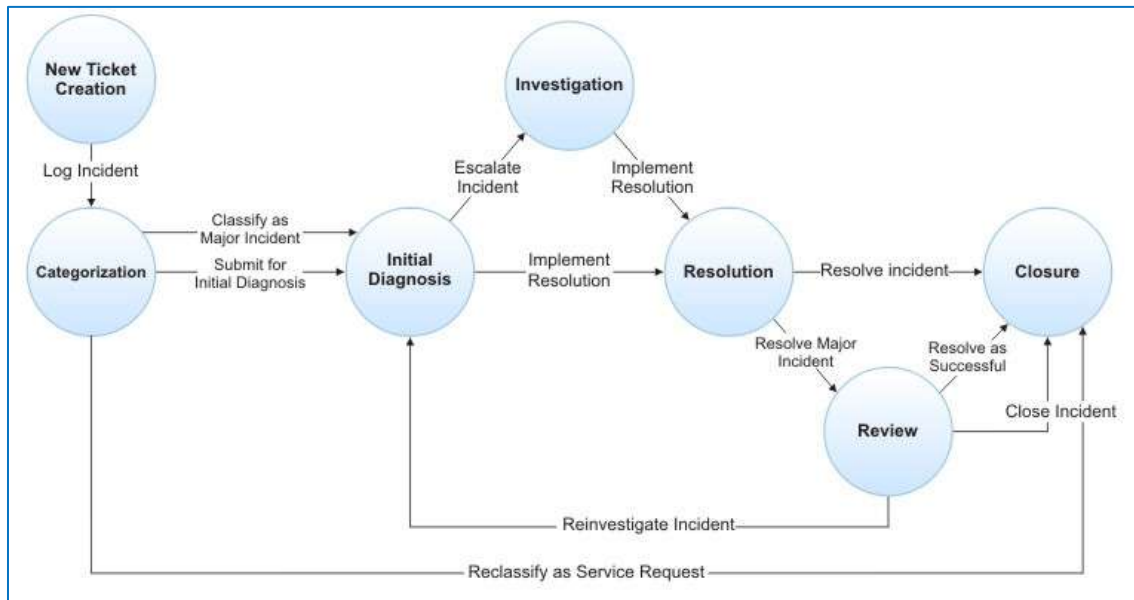
Ticket Phase

The processes followed for managing the entire spectrum of requests handled by the Service Desk forms the mainstay of Service Desk Operations. Each type of request would have its own unique requirement and would therefore mandate its own unique workflow for managing the Service Delivery Process.

Nimsoft Service Desk provides workflow features to manage the Life Cycle of all tickets from creation to closure. The Administrator can configure different workflows for different type of tickets logged in Nimsoft Service Desk and can also make modifications to the workflow based on the nature of the request.

ITIL recommends that a ticket passes through a systematic process, where the ticket moves to different status and phases. Phasing is used to help segment and define the steps in a given process workflow. During a ticket life-cycle, the ticket passes through different phases.

For example, an Incident that is assigned to an individual or support group could be in Investigation and Diagnosis Phase. The default configuration of Nimsoft Service Desk defines some actions that transition tickets from one Phase to another; while other actions could transition tickets within a phase.



Definition of a phase, progression of the ticket through different phases, etc. can be configured for different tickets as per the conventions in the user's organization. Also, the concept of Phase is not imposed. Phase on tickets can be enabled or disabled by setting the appropriate slice configuration parameters.

Ticket Status and Reason Code

Ticket Status

A ticket goes through a life-cycle from the time it is logged (and assigned a ticket number) to its closure. Ticket Status refers to the current stage of the ticket in its life cycle. Nimsoft Service Desk allows movement of a ticket through different statuses like:

- New
- Queued
- Active
- Pending
- Resolved
- Closed

These values are fixed and cannot be customized for an organization. The progression of the request through these different statuses is controlled by the workflow that is defined by the administrator.

It is not necessary that the ticket moves through each status in a sequence. The movement of the ticket from one Status to another is controlled through the current status of the ticket and its current state in the workflow.

Ticket Reason Code

The movement of a request into any given status, either by the agent or by an auto-route, has to be guided by some set reason. This reason can be seen by viewing the “Reason Code”. The Reason Code depicts why a ticket is in a particular status. For example, a ticket status could be “Pending” with the Reason Code as “Pending Vendor Information”.

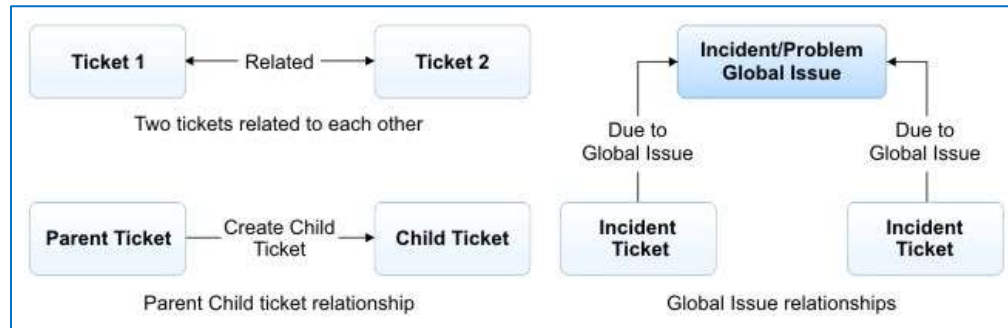
The Reason Code and how they are associated with a Ticket Status is controlled by the workflow that is defined by the administrator. There is no limitation on values for Reason Code field. Administrator can add more reason codes and use them in configuring matching conditions and Set fields of workflow entities (Action Options, Auto routes, etc.) as per the needs of the organization.

Ticket Relationships

Relationship refers to how two entities interact with each other and how they affect each other. Nimsoft Service Desk allows creating and managing some critical relationships between two or more entities in the IT Service and Service Delivery domain. Nimsoft Service Desk allows relationship between tickets and Configuration Items.

One Ticket could be related to other tickets or it could be related to one or more Configuration Items. Similarly, one Configuration Items could be related to other Configuration Items and could be related to one or more tickets.

In Tickets, an Incident Ticket may be related to other Incident Tickets or may be related to a Global Ticket. Similarly, a Change Ticket may have been created out of a Problem Ticket to resolve the Problem and hence has a Parent-Child Relationship with the Problem Ticket.



Maintaining such relationship between tickets allows for some of the actions to be carried over from the Parent Ticket to the Child Ticket or from a Global Ticket to all related tickets. This in turn ensures that all open issues related to each other are handled appropriately minimizing human intervention in these actions.

Ticket Templates

In the context of IT support, there are several oft repeated requests like request for permissions to use or access a resource, reporting unavailability of some IT object or Service, or request for some standard modification like upgrade to a latest version of software. For such frequently requested tickets, Ticket Templates can be configured and made available to users.

Ticket Templates offer a standardized information collection system for requests that can be anticipated by different sets of users. It also facilitates effective application of auto-routes, such as having a ticket assigned directly to a specific group/individual rather than the ticket getting assigned by default to the Level 1 Support and thereafter moving to the appropriate queue.

Ticket Templates are pre-populated with baseline information and contain place-holders for additional information. These Ticket Templates, per ticket type, can be made available to Self-Service Users and/or Service Desk Agents by enabling permissions for access to the users, support group, or role.

A ticket template can be configured by setting field values for standard ticket fields, as well as providing values for Custom Fields on tickets. When a user accesses the ticket template, the set field values are populated in the ticket fields as configured by the application administrator.

Based on the set field values, auto-routes could get applied to the ticket, action options become available on the ticket, and certain fields get marked as required fields.

Using Ticket Templates eases the process of ticket creation for standard requests. Task Ticket Templates can be used for Task Groups and Task Flows.

Ticket Workflows

A workflow is a sequence of connected steps taken towards achieving a desired objective or goal. It depicts the progression of an activity from one step to another towards achieving the final purpose of the target activity.

At each stage of the workflow, an individual or set of individuals assume ownership and responsibility for the activity being undertaken.

Sound Workflows also ensures the ability to bring in complete or partial automation of a business process. Documents, information, or tasks are passed from one participant to another for action according to a set of procedural rules established by the workflow.

Establishing a workflow allows reliability and repeatability to a set of activities. Well implemented Workflows result in:

- Process Standardization
- Increased Productivity
- Reduced Response Time
- Reduced Errors
- Improved quality of Service and Support

Nimsoft Service Desk allows you to configure workflows based on ITSM Best practices and guidelines wherein you can set the progression path of a ticket from one stage to another.

The Nimsoft Service Desk workflows allow you to guide Service Desk Agents to progress a ticket through possible alternative actions based on the ticket attributes. You can configure workflow action for each ticket type, where based on ticket matching conditions, action options become available on the ticket.

The Service Desk Agent working on the ticket can take an appropriate action from the available options and progress the ticket further in its life-cycle.

You can configure a specific Change Management Process, where a ticket moves through an approval process and is reviewed and approved before implementation.

Workflow actions can be automated by applying actions like Auto-Create Tasks, auto-assign action, and by defining action on success and action on failure of a task ticket. Ticket workflow automation is facilitated via auto-routes and action options.

Work & Time Tracking

Worklogs are manual entries in the ticket to record information that is relevant or significant to the issue. This information is not automatically captured by Nimsoft Service Desk.

Information such as findings on an issue that is being worked upon, telephonic discussions related to the issue, or issue resolution can be logged as Worklogs in the ticket.

While most Worklogs are updated by the Service Desk Agents, a Self-Service User can also add a Worklog into the ticket to give additional information related to the request. The Service Desk Agent can use the Worklog to communicate information related to the ticket (like work done on a ticket) to the customer.

The Service Desk Agent has the ability to share or hide Worklogs being added to a ticket by marking the worklog as Client Viewable and thus making it visible to the requestor. For internal communications within the team, the Agent can disable the Client Viewable field, thereby restricting visibility of the Worklog.

Nimsoft Service Desk also allows Worklog updates to be sent as Email to identified recipients. The agent can check the Send as Email option before saving the Worklog to initiate the action of sending the Worklog as an Email. This further reduces the Agents' need to send out specific communication to the requestor or other stakeholders regarding any work done or update on the ticket.

Nimsoft Service Desk allows the capability of tracking the time spent on working towards resolving or closing each ticket. Each individual Service Desk Agent who works on the ticket can log the time spent on the ticket. This information can be filled into the Worklog Section of the ticket.

Nimsoft Service Desk also maintains an automatic total of all the time spent on the ticket by calculating time spent per worklog. The total time spent can also be seen on the ticket.

Tracking time in this way allows the managers and supervisors identify the activities that occupy support most; and also help them keep track of the time being spent by each agent on working on the tickets thus bringing visibility to the time spent on support activities.

The Administrators can choose whether they wish to adopt time tracking on tickets or not.

Request Handling Process

A Self-Service user can log requests using either a phone, email, or the Self Service interface of Nimsoft Service Desk Application.

For repetitive, common requests, the administrator can provide Ticket Templates and set up Auto-Routes inside the application. When these requests are logged, they get auto assigned to specific Groups / Individuals based on the auto-route that gets applied. Other requests are assigned by default to a Level 1 group.

If the request is for information or service that can be delivered by the Level 1 Support team, the request is serviced and the ticket status is set as resolved by the Level 1 support person. The Level 1 support also takes decisions as to whether the request is to be reclassified as an Incident or a Change.

If the request cannot be handled by the Level 1 support, it gets escalated to a Level 2 support group. This group then works towards issue resolution and sets the ticket as resolved upon completion.

If the request requires assignment to an identified person or group, the request gets manually routed accordingly (if no auto-route has been designed for direct assignment to that person/group).

Each support individual or group which holds the request, works towards resolution of the request as per the workflow set by the customer's Nimsoft Service Desk Administrator.

While some requests may be worked upon as independent entities, other requests would require creation of child or task tickets while yet others could get related to other tickets or be related to a global ticket. When the request has been fulfilled, it is set as resolved and gets closed as per the workflow defined by your Nimsoft Service Desk Administrator.

Notification of ticket creation, assignment, worklog additions, and any modification to the ticket can be sent out to the requester by the application directly.

The requestor can keep track of updates and progress on his/her request via the notifications sent out by the application or by logging into the Self-Service Interface of Nimsoft Service Desk Application.

The request handling process is managed by configuring auto-routes and workflow actions for the ticket.

Special Function

A workflow action option is designed to guide the Service Desk Agent towards the next set of actions that can be taken on a ticket given the current stage and state of the ticket. Workflow actions act as a check to ensure that the processing of the tickets is as per the desired workflow pattern.

The concept of Special Functions has been introduced to enable a workflow action to trigger off an automatic action on the ticket before an action is performed.

Special Function option can be used If an action option requires achieving something more than merely setting values of ticket fields through Set Fields tab.

For example, say “create a child Incident ticket” or “Submit change request for approval to approvers”, special function is required to be added to the action Option. The special function automatically triggers additional chores to be performed for the Action Option.

When configuring an action option, you can choose a special function to be executed with the Action Option. Some examples of Special Functions are:

- Check for Open Tasks - can be used to check resolution of task tickets related to a Global Issue when parent ticket is resolved.
- Auto-Create Tasks - can be used to create task tickets at a specific point in the ticket life-cycle.
- Submit for Approval - can be used to automatically add approvers and reviewers to the ticket.
- Withdraw from Approval - can be used to withdraw ticket from approval process.

Other Special functions can be used to Delete tickets, create child Incident, Problem or Change tickets, or other assignment related actions.

Set Fields

When designing the workflow for a ticket, the administrator identifies the stages through which the ticket will progress and the conditions on the ticket at which an auto-route or workflow action option or approval group gets applied to a ticket.

When a workflow action, auto-route, or approval group gets applied to a ticket, it needs some changes of the field values as required by the workflow design.

Set Fields is a feature available to the Application Administrator while configuring Action Options, Auto-Routes, or Approval Groups for managing the workflow on a ticket.

The Application Administrator can select the attribute(s) and specify what value each attribute should assume after the execution of the Action Option or Auto Route or a step of change Approval Process.

Auto-Route get applied to a ticket based on Matching Conditions and the ticket can get assigned to an identified group as per Set Fields without any delays.

Configuring Set Field values to be modified upon execution of an action or application of an auto-route, aids in further guiding the Service Desk Agents working on the ticket to process the ticket as per the workflow design.

Set Fields can also be used to configure Ticket Templates; wherein field values like Status, Reason Code, Description, Priority, etc., can be pre-configured to be displayed when the ticket template is invoked by a user.

Setting field values on the ticket template aids the user by expediting the ticket logging process. Auto-Routes can get applied to the ticket based on the set-field values, and the ticket can get assigned to an identified group without delays.

Core Application Concepts

Communication Logs

Users of Nimsoft Service Desk interact with the application via email. Emails sent to the IT Support (on IDs configured for a Customer Slice/Tenant) get logged as a ticket in the Customer Slice/Tenant's instance of the application. Email notifications are sent out by the application when pre-defined actions are taken on the tickets.

Communication is exchanged between Nimsoft Service Desk and the users of the application for all transaction performed while using the application. A history of all communication sent out and received by the application is maintained as Communication Logs within the application.

The communication related to a specific ticket can be seen from the Activity Tab of the ticket. Here, the Service Desk Agent working on the ticket can view details of all incoming and outgoing mails. This includes automatic notification triggered by a workflow action or an auto-route as well as any manual communication sent or received.

Self-Service Users can view communication history in the Worklog section of the ticket. Based on configurations managed by the application administrator, they can view information on both Incoming and Outgoing emails, or just incoming mails.

Application Administrators can access communication history of a specific ticket from within the ticket. They can also view information on all incoming and outgoing communication logs from the Search Communication link under Administration Utilities.

Application Administrators can draw out details of all communication by selecting the search conditions on the basis of which they wish to filter the search. They can view details such as sender, recipients, Status (Queued, Delivered, Scheduled, Failed, etc.), and view details of the communication being sent.

The application administrator can also delete a schedule communication, if so required.

Communication Logs give the application administrator a visibility over communications to and from users of IT Support.

Communication Templates

Nimsoft Service Desk can be configured to send out email communication to intended recipients in a variety of contexts. Users receive notifications from the system regarding transactions on a request they have raised.

They also receive communication regarding tickets submitted for approval or a Service Feedback schedule. Service Desk Agents can also manually send out communication from a ticket.

To facilitate appropriately structured, uniform, and timely communication to all stakeholders related to a ticket, the Administrator can create Communication Templates and make it available to different ticket types.

Communication Templates are pre-configured email templates, with the standard message subject or body text being created by the administrator. Communication templates can be used for both automated notifications and for manual communication by a Service Desk Agent.

For variable information that needs to be pulled out from the context of the communication, (like Ticket or Service Feedback Schedule), fields from the form can be inserted as place holders. The recipients of the communication can also be pre-configured, and details will be pulled from the context of the communication.

Communication Templates can be configured for different action on the ticket during the ticket life-cycle. When configuring a workflow action or auto-route, communication templates can be associated with the action. When the action is executed, automatic notifications are sent out to intended recipients identified in the communication template.

Service Desk Agents working on a ticket can also manually send out communication from a ticket. They can use pre-configured Communication Templates for these communications.

Agents can also schedule email communication to be sent out at a future date and time. If they schedule a communication using a template, they can set up a flag for the variable information to be updated at the time of the communication dispatch.

A range of pre-configured Communication Templates, with standard notifications on common workflow actions or system notifications, are made available by default as System Defined Communication Templates. The content of these templates can be modified as per your requirements.

Access to Communication Templates can be controlled by permissions assigned to users, support groups, or roles.

Using Communication Templates to send out notification to all stake-holders ensures that all communication regarding the transaction is done in a timely manner, without manual intervention. Also communication can be comprehensive, standardized and uniform - irrespective of the actual sender's ability to communicate precisely.

Dashboard Charts

Dashboards enable users to access real-time information on performance against established Key Performance Indicators (KPI). These key indicators ensure accountability and efficient functioning. Dashboards provide the business perspective in a very clear fashion and help to align us with strategic goals.

Nimsoft Service Desk provides a collection of individually tailored KPIs such as Ticket Aging, performance related to SLA compliance, etc., to create dashboards for different user roles. As application administrator you can define KPIs and group them together to create various types of dashboards.

Providing dashboard access to Service Desk Agents allows them to see their own tickets as well as group tickets while keeping a close eye on resolution rate and SLAs. Service Desk Agents get an eagle's view into the overall health of the Service Desk.

By enabling the generation of Dashboard charts to view ticket trends allows monitoring and better control of service desk operations.

Defined Searches

Search is a functionality that allows users to pull out existing records from the application. Searches can be used by Self-Service Users, Service Desk Agents, and Administrators.

Users of Nimsoft Service Desk have access to Global Search (where records can be searched by using matching Key words), Advanced Search (where users can specify search parameters), and defined-search (where a pre-defined Search Query is made available).

The Defined Search functionality enables you to construct a search query for more specific search needs and save the query to be executed whenever needed. Based on queries frequently used by Service Desk Agents, you can configure an SQL query to include or exclude specific data elements and search for data most relevant in the context of the search.

Defining Searches reduces the efforts needed by Agents to pull out data from the system and enables them to access appropriate data when needed. As the output is designed to be more specific, the effort of sorting through unwanted data is reduced.

Defined Searches are also a pre-requisite for configuring Charts. Charts pull out data queried by a defined search and render that information in the form of a visual (rather than as a text data output). Based on the refresh interval set in the chart, the SQL query of the defined search is executed again, and fresh data is displayed.

Thus, configuring defined searches enables users to view interactive data real time as well as allows users to draw out identified data for further analysis or use.

Emails Based Working

Nimsoft Service Desk can be configured to enable logging of requests via email; and for notifications to be sent directly from the relevant form in the application. Email interactions and updates into relevant forms can be set up for Tickets, Service Feedback, SLA Escalations, and Approval Notification.

In addition to interacting with Nimsoft Service Desk , a user can also interact by sending in an Email to a Support Email address. The user can log a new request via Email or reply to a notification received from Nimsoft Service Desk. In this way, requests can be updated via Email.

The email ID of the requester is matched with the existing records and a ticket is created with the sender of the email ID being added as the requester of the ticket. Based on matching conditions or default assignment group identified, the ticket gets assigned to an appropriate workgroup for appropriate action.

Service Desk Agents can send an email from the ticket to identified recipients and also choose to send their worklogs as emails to identified recipients. The Nimsoft Service Desk Administrator can also set up notifications to be sent out by email on certain actions on tickets, like status changes, SLA Target violations, etc., without any intervention from the Service Desk Agent.

The incoming Email is analyzed for information of the Sender and the Subject of the message. Based on presence of specific words or phrases, Nimsoft Service Desk either creates a new Service Request or finds the existing ticket to which the message should be appended.

Emails can also be sent with predefined XML format for Message Body and Nimsoft Service Desk processes these Emails as configured for the specific XML format. This feature is useful for other applications to interact with Nimsoft Service Desk.

Global Search

Global Search allows users to search Nimsoft Service Desk for records stored in their instance of the application. The search text specified could be numeric, alpha-numeric, or could use other characters.

Based on user specified text, the application will search through predefined information areas of Nimsoft Service Desk and bring up direct links to relevant entities. These areas include Organizations / Sites / Locations, Contacts, Support Groups, Tickets, Solutions, Navigation Help, etc.

The user can click on the link to reach the details of the selected record. This allows the user to search their instance of Nimsoft Service Desk for the tickets they have logged (or based on Permission - tickets logged by others in their organization) for solutions made available to them by the Application Administrator.

Global Search takes into consideration your log-in credentials, and will list only those items that you (or the support group(s) that you are part of) have been granted permission to view.

This means that if your Nimsoft Service Desk Administrator has restricted access of a particular Solution record or Configuration Item record for your support group that entity will not be displayed in your search results.

Global Search is a functionality that can be used by Self-Service Users, Service Desk Agents, and Administrators.

Matching Conditions

The 'Condition' of a ticket is identified by the values in the various fields of the ticket. For example, the value in the Status or Phase field of a ticket gives an indication of which stage of the ticket life-cycle the ticket is at. Similarly, value in fields like Priority, Impact, Urgency, etc., indicate the prioritization condition of the ticket.

Actions can be taken on the ticket based on the current 'Condition' of the ticket. Matching Conditions is a concept that allows you to control what action can be allowed on a ticket based on the current Condition of the ticket.

In Nimsoft Service Desk, Matching Conditions can be configured for Auto-Routes, Action Options, Approval Groups, and Defined Searches.

While most fields are available when configuring Matching Conditions, the most useful attributes for creating a Matching condition are:

- Status Related - Status, Reason Code, Phase
- Prioritization Related - Priority, Severity, Urgency, Impact, Business Criticality
- Categorization Related - CCTI
- Requester Related - Requester, Requested for, Requester Organization, Site, Location

Matching Conditions can be configured on Auto-Routes, whereby a ticket that matches the conditions of the Auto-Route, bypasses default routing rule specified in the Slice Configurations and gets routed to an identified Support Group.

Similarly, based on Matching Conditions different Action Options get displayed on a ticket at different stages of the ticket life-cycle. Approval Groups get associated with a Change Ticket based on Matching Conditions on a ticket.

If no Matching Condition is specified for an Auto-Route, Action Option, or Approval Group, the action gets applied to all tickets of the Related Ticket Type.

Automation and process control can be achieved by using the concept of Matching Conditions.

Notification

Notification is a message sent to an Individual or Group when a pre-defined situation or event occurs. For example, notification is sent out to a requester when an email sent to Support results in a ticket being logged.

Similarly, based on workflow configurations, when a Service Desk Agent changes the status of the ticket or adds a Client Viewable worklog, notification will be sent to the requester of the ticket.

Notifications are sent out to Change Approvers or Change Reviewer when a ticket is submitted to them for Approval or Review. The recipients can respond to this notification and update the ticket via the email response.

Notifications are also sent out to participants in a Service Feedback process. An Email notification, with a link to the Service Feedback survey gets sent to the participants identified in the schedule.

The recipients can respond to the Survey as appropriate. The response from the identified respondents is sent back as notification to a concerned, identified recipient of the feedback results.

Users also get automated notification from Nimsoft Service Desk about password resets.

Thus, system generated notification can be configured to be sent out by the system on the occurrence of a pre-defined activity.

Permissions

Permissions is a concept used to control access of users to features and functionality of Nimsoft Service Desk as well as to perform certain actions in the application. The Application Administrator manages the ability of a user trying to access Nimsoft Service Desk Application and the ability of a logged in user trying to undertake an operation using the application.

Permissions are associated with the following entities in the application:

- Navigation Menu: Modules and Links visible in the Navigation Menu
- Toolbar: Items visible in the Toolbar of Ticket forms, CI records, and Knowledge Articles.
- Report: Related to Tickets, Configuration Management, Knowledge Management, and Service Feedback
- Dashboards and Charts: My Dashboard link and individual Charts and Dashboards.
- Defined Searches: Related to various Ticket Modules
- Workflow Actions: Availability of an Action Option in the Take an Action option on tickets
- Ticket Templates: Related to different ticket types
- Communication Templates: Related to different ticket types
- Knowledge Base Articles: Access to Active and Approved articles

A user can be granted permissions to an item directly or permissions can be granted to the Support Group or Role. All users of a Support Group or Role inherit the permissions assigned.

If permission to an item or record is not enabled, the logged in user will be unable to view the item or record and will therefore be unable to use it.

Primary Organization

Nimsoft Service Desk allows customers to configure records for more than one Organization including Service Users, Service Providers, and Vendors, each with its multiple sites and locations.

Contacts from these organizations can be created in Nimsoft Service Desk. Contacts could be made part of more than one organization. This permits them to view ticket data of all organizations they may be required to support.

Some of the elements in the Nimsoft Service Desk GUI visible to the logged in user, like display of Organization's logo, inclusion or exclusion from Service Feedback Forms, and ability for Self-Service Users to view their organization's tickets, are associated with Contact's Organization.

To limit these "organization based functional features", one Organization has to be set as the Primary Organization for the contact. Based on this preference, these features get applied. While the contact may be able to view ticket data of other organizations on Home Page, the default view will be based on the Primary Organization.

Administrators set up a Primary Organization for the contact and this can be modified on need basis by the Administrator. Only one Organization can be set as a contact's primary organization at any time.

PIN Authentication of Contact

Service Desk works on requests from registered users of IT Services and Support. Often, these requests for support are logged via emails or via Phone Calls to the Service Desk.

Some requests logged with support, especially Change Requests, could require authentication of the requester. This becomes especially important when the request is raised via phone; the Service Desk Agent needs some way of validating the requester.

To facilitate such authentication, contacts in Nimsoft Service Desk can be assigned PIN Numbers. The PIN Number of the contacts can be accessed along with other details of the contact in the Contact Records stored in Nimsoft Service Desk.

PIN Number Authentication allows the Service Desk Agent, who is working on the request, some degree of control in carrying out pre-approved/standard changes based on the workflow designed for such activities or tasks.

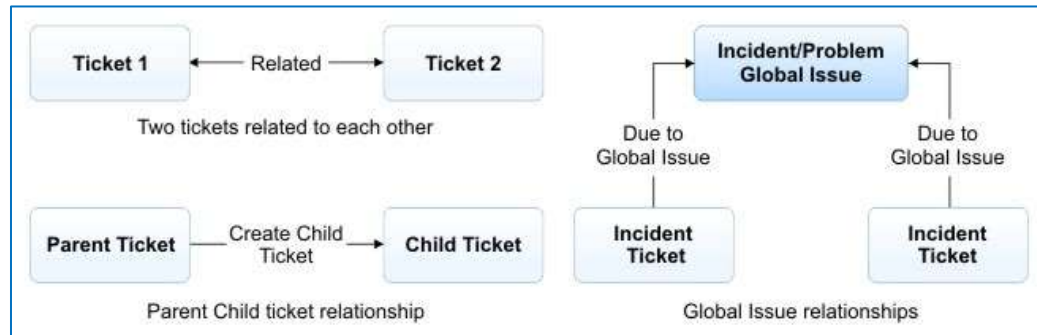
Relationships

Relationship refers to how two entities interact with each other and how they affect each other. Nimsoft Service Desk allows creating and managing some critical relationships between two or more entities in the IT Service and Service Delivery domain including Tickets, Configuration Items, and Contacts.

A ticket logged in the application could be related to other tickets. One possible relationship is that of a Parent-Child relationship between the tickets. For example, consider that a Service Request is logged by a requester.

The Service Desk Agent working on the ticket analyzes the ticket and classifies the ticket as an Incident Ticket. The Agent executes the action of Create Incident from the Service Request.

The Incident Ticket is created as a Child to the Parent Service Request. Thus a Parent Child Relationship is created between the two tickets. A similar Parent Child relationship also exists when Task Tickets are created to execute activities towards resolution of a parent Service/Incident/Change/Problem ticket.



Besides Parent Child relations, where the Service Desk Agent feels that a ticket is related to other open tickets in one or another way, the Agent can relate the ticket from the Related Tickets tab on the ticket.

Where a ticket is reporting an issue that is affecting several CIs or which has resulted in several other tickets being logged, the issue can be marked as Global Issue and the relevant tickets can be related to the Global Issue. Thus, the tickets become related to a Global Issue and actions on the Global Issue can be transmitted to the related issues.

Relationships can be established between two or more Configuration Items in different relationship domains (See CI Relationships). Similarly, a Configuration Item can be related to one or more contacts in different capacities, like owner, user, support provider, etc. When a ticket is logged for a Configuration Item or because of a Configuration Item (CI), the CI can be related to the ticket.

Relationships can also be applied to Knowledge Base Articles. A KB Article can be related to a Configuration Item, Categorization (CCTI of CI), Organization, Site, or Location. Configuring such relationships on Knowledge Base Articles facilitates effective searches for solutions to tickets.

Reporting

Reports are used extensively to analyze performance, draw trends, and predict behavior based on past performance. Nimsoft Service Desk enables users to access a wider range of reports as per the reporting needs of the organization.

Nimsoft Service Desk provides a range of out-of-the-box reports related to Tickets, Configuration Items, Knowledge Base Articles, and Service Feedback Surveys. Ticket related reports can be drawn to view performance in terms of SLA compliance, Ticket volumes, Ticket Aging, etc. Ticket related reports can be drawn for each ticket type, as required.

A collection of all available reports can also be accessed in the Trends and Metrics Module. In this module, reports are grouped under different links and each link contains a list of reports that have been grouped under it. All reports related to a module can be also accessed from the Reports link within the module.

Access to all reports is controlled via permissions. Agents can be granted permission those reports that they need to view or use. Control to view the Trends and Metrics module can also be controlled via permissions.

Scheduled Hours & Holidays

Increasingly, IT Operations are spread across geographically diverse regions and Service Support is offered from different locations across the globe. Consequently, Support Groups within an organization could be working at different time periods distinguished by the Time-zone in which they operate.

Schedule Business Hours refers to the time period between which an IT Service or an IT Support Group will be available. Usually, an IT Service or Support Group will be available during schedule business hours. Availability of an IT Service or Support Group can also be affected by Holidays observed by the organization.

While in some organizations, Service Desk Operations are established as 24X7 operations, in other organizations, Support is available between identified business hours. Like Support Groups, while some IT Services could be available 24X7, other services could have a fixed availability schedule.

To better manage factors like Ticket routing and SLA monitoring, Business Hours schedules can be configured for the Support Group. A Holiday Group can also be associated with the Schedule, indicating unavailability of the Support Group. Availability schedule can also be configured for an IT Service, which defines the time period at which an IT Service will be available; and holidays when the IT Service will be unavailable.

The Schedule indicates that the support group or IT Service will be available only during the stipulated business hours and will not be available outside the business hours or on identified holidays. Multiple Schedules can be associated with a Support Group or a Configuration Item categorized as Service.

A Schedule can also be associated with an Auto-Route, which controls the time duration during which the auto-route gets applied. You can use this to manage routing of tickets based on Support Availability schedule. Auto-Routes can also be configured to be specific to holidays, whereby tickets get routed per the auto-route only on holidays.

Scheduled Activity

Service Desk Agents working at the IT Support or Service Desk work mainly against requests from the end-users which are assigned to them in the form of tickets. Much of the work done is reactive in nature as the need for IT support cannot be cleanly predicted.

However, there are some tasks that Service Desk Agents would be required to take on as part of routine maintenance of the IT Objects and devices. These could be tasks such as taking data backups, monitoring logs, preparing reports, or other such tasks which would form part of the Service Desk tasks.

For such tasks which are regular, usually done on a fixed date, and often at a fixed time, Nimsoft Service Desk allows configuration of Schedules. As per the schedule, Tickets get created and assigned to the Schedule Owner at the scheduled time.

A Schedule can be configured to create appropriate tickets based on a specified ticket template for such activities / tasks. The tickets are assigned to identified individual or group at fixed intervals. The administrator can specify what time the ticket shall be created and set a recurrence pattern for repeated creation of the ticket.

Once created, these tickets will get automatically assigned to the specified individual or group for processing. This saves the agent the need to maintain a separate schedule for routine tasks; and gives the administrator greater control of these routine operational activities.

Self-Service User Interface

Self-Service Users are usually the requesters of IT support or service. They are concerned mainly with resolution of the issue they are facing or getting the information that they need to use the IT Service made available to them; they are not too concerned about the mechanism of processing the request.

Self-Service Users have limited interaction with Nimsoft Service Desk Application, using it mainly to log their own support requests and monitor progress of their own requests.

For such contacts, who are mainly requestors of service and play an external role in the IT Support, Nimsoft Service Desk provides a simplified Self-Service User Interface with limited functions and permissions.

The Self-Service User Interface allows users to log on to the application to log their requests, view progress of their request from the application interface, and add notes to their requests via a worklog on an existing ticket.

When the Self-Service User is a Change Approver, s/he can view the change ticket that is submitted for approval and Approve or Reject the change.

As Self-Service Users are usually participants in the Service Feedback process, they can view any open Service Feedback Schedule where they are identified as participants and they can submit their feedback from within the Self-Service User Interface.

Self-Service Users can also access useful information on Known Outages, News and other Informative Articles, Frequently Asked Questions, and access Knowledge Base Articles. They can use this information to solve their own IT related questions and thus reduce their dependency on Support.

The Self-Service Interface gives the Self-Service Users 24X7 access to the IT Services and Support.

Configuration Parameters

Service Desk operations are managed differently in each organization. While some customers would want certain features, other customers would not wish to enable a given feature or would want to use it in a different way.

Configuration Parameters is a way of enabling the Application Administrator to control how the application is used in their organization's context.

Nimsoft Service Desk allows individual customers to manage a wide range of the application functionality to suit the distinct need of their organization. To enable the application administrator to enable or disable a feature or functionality or modify a function in some limited way, Configuration Parameters are made available on the interface.

Each Configuration Parameter has a parameter with specified values to define its role and behavior. A parameter value can be in the form of a Boolean variable, a number, an URL, a list depending upon the kind of Role performed by the Parameter, etc.

The Application Administrator can customize a slice by selecting an alternative variation for the Slice Parameter value to suit the needs of their organization.

New Configuration Parameters are added to the application when any new features that could impact backward compatibility, is introduced. By setting the Slice Parameter value appropriately, the Application Administrator is given the flexibility of managing IT Operations as per the organizational requirements.

Sort Order

Sort Order is the value that indicates the order of precedence of an entity or a record in Nimsoft Service Desk. An entity or record with lower sort order takes precedence over a record having a higher sort order. The concept of Sort Order is applied on all forms where applicability of the action or visibility of an option has to be controlled.

For example, consider two attributes that are used for creating custom fields on tickets - 'Employee Name', with Sort Order 1 and Employee Code, with Sort Order 3. If both attributes are used on a ticket template, the field Employee Name will be displayed first on the form followed by the field Employee Code.

Sort Order is applied to the following forms in Nimsoft Service Desk:

- Attributes
- Action Options
- Auto-Routes
- Task Groups
- Defined Searches
- Values (visible in the drop-down lists on ticket fields)
- Navigation Menu
- Toolbar Options
- Report Configurations

When applied to records such as Attributes, Defined Searches, Navigation Menu, Toolbar Options, Report Configurations, and Action Options, the Sort Order controls the order of display of an entity in the relevant forms or action links.

Sort Order becomes important on Auto-Route instances when a ticket condition matches the Matching Condition for more than one Auto-Route. In such an instance, the Auto-Route with the lowest Sort Order gets applied to the ticket.

The Concept of Sort Order is also applied to Task Flows. Task tickets or Task Groups get created as per the sort order specified. A Task/Task Group with lower Sort Order gets created first and when the Task/Task Group is complete (resolved or closed), the Task/Task Group with the next Sort Order gets initiated.

Thus, Sort Order helps control how a record or item functions in the application.

VIP User

Often, organizations have certain users whose requests need to be prioritized differently and handled in a specific way. Such a contact would generally be considered a VIP User and requests logged by this person would be given more importance or be treated with higher priority.

Nimsoft Service Desk allows for contacts to be marked as VIP users. When setting up the contact record in Nimsoft Service Desk, identified users can be marked as VIP Users. The VIP user flag can be set for all type of users (Self-Service, Service Desk Agents, and Administrator). The VIP flag can also be set when bulk importing contact records into your instance of the application.

When a VIP user is selected as “Requester” or “Requested For” during ticket creation, a message is displayed indicating the requester is a VIP User. This guides the Service Desk Agent in according appropriate priority to the request.

Also, the column in the ticket list containing the request from a VIP User is highlighted in a different color from the other user’s request. This further helps distinguish VIP users and prioritizing their request appropriately.

Chapter 3: Application Functionality

Introduction

The features and functionality available to different users are explained in the introduction section of each module. This section provides you a holistic view of the features that are available to both Self-Service Users and Service Desk Agents. It also provides an overview of what the application administrator does in managing or enabling a feature or functionality.

The functionality has been grouped into Ticket Related Functionality and Non-Ticket Functionality. You can read the details about how each different use types access and use a functionality.

Ticket Related Functionality

The tables below identify the key functionality offered by Nimsoft Service Desk and how the functionality is made available to Self-Service Users, Service Desk Agents and Application Administrator.

Both Self-Service Users and Service Desk Agents access the Ticketing functionality listed below, although the scope of their interaction with the functionality differs.

Ticket Logging

All new requests for support are logged as Tickets in Nimsoft Service Desk. Ticket logging is a functionality accessed by all users.

Features	Ticket Logging
Self-Service User	Self-Service Users can log tickets directly via the Self-Service User Interface or via emails sent to Support. Self-Service Users can also view all ticket that they have logged (or have been logged on their behalf) from the SSU interface.
Service Desk Agent	Service Desk Agents can log tickets on behalf of a requester, or proactively log a request if an issue is identified. All tickets logged by end-users get assigned to Support Groups based on default Support Group specified, or specific Auto-Routes that get applied. They can view details of all tickets assigned to them individually or their Support Groups and work further on the tickets.
Application Administrator	Application Administrators can specify default assignment groups per ticket type by updating required Slice Configurations and configure specific Auto-Routes and workflow actions to be associated with a request when it is logged. This includes configurations for tickets logged via the web applications or via email.

Ticket Templates

Ticket Templates, with relevant pre-populated information, are used for creating and submitting tickets with minimal additions. The ability to access these templates is managed by the administrator.

Features	Ticket Templates
Self-Service User	Self-Service Users can use Ticket Templates made available to them in the Request Catalog. They can choose the template that best fits their request need; make minimum required addition or changes; and use it to submit the request. As much of the key details are already filled in, the Self-Service Users save time in submitting the request.
Service Desk Agent	Service Desk Agents can use Ticket Templates, made available for different ticket types, to log a new ticket. Tickets logged by Self-Service Users, using a ticket template, can also get assigned to specific Support Groups based on configurations managed by the administrator.
Application Administrator	Application Administrator configures Ticket Templates by setting information in the various ticket fields and providing a format for the information to be gathered. Custom Fields can also be added to ticket templates. Certain fields can be marked as Required Fields, to ensure essential details are filled in. The Administrator manages access to the Ticket Templates by granting permissions to contacts, Support Groups, or roles.

Custom Fields on Tickets

Custom Fields enable soliciting and gathering additional details over and above the standard ticket fields when a ticket is logged.

Features	Custom Fields on Tickets
Self-Service User	Self-Service Users may see Custom Fields on tickets in the section called Additional Information when they log a ticket using templates from the Request Catalog. Some of the fields could be marked as RequiredFields. They can use these fields to provide the required additional information.
Service Desk Agent	Service Desk Agents can see a tab on tickets called Additional Information Tab. This tab contains Custom Fields configured by the administrator for the ticket. Service Desk Agents can update essential information into the Custom Fields for processing of the request. They can also use details on custom fields in advanced search for tickets.
Application Administrator	Application Administrator configures Custom Fields on tickets. They determine which templates will have custom fields; they group custom fields into sections, if appropriate; they determine whether the custom field is to be marked as Required Fields; and determine if the custom field is to be visible to Self-Service Users. They can also make a Custom Field or individual attributes on a field inactive.

Ticket Classification

Ticket Classification enables appropriate handling of the ticket by an identified support group, and reduces effort in locating resources needed to work on the issue.

Features	Ticket Classification
Self-Service User	Self-Service Users do not classify tickets. They do not log different types of tickets for different types of requests; although in the back end, a request may get classified as an Incident or Change.
Service Desk Agent	Service Desk Agents classify tickets into Service Request ; Incident, Problem or Change Ticket; depending on the nature of the request. They may also need to create a Child Ticket from an original Service Request if an existing ticket needs reclassification. They may further classify a Change Ticket based on Change Type or a Task Ticket on Task Type, etc. Such classification is done to ensure appropriate handling of the ticket by the right team or Support Group .
Application Administrator	Application Administrator configures Workflows that enable effective routing of tickets based on the Ticket Type and other classification. They also configure workflow action options that enable Service Desk Agents to create Child Tickets for re-classification.

Ticket Categorization

Ticket Categorization, by applying appropriate CCTI enables appropriate handling of the ticket, effective assignments, and effective search for solutions from the Knowledge Base .

Features	Ticket Categorization
Self-Service User	Self-Service Users can categorize a ticket by choosing an appropriate option in the Type field of the ticket to classify a ticket, if this field is enabled by the administrator. This field could be pre-populated in ticket templates made available to Self-Service Users.
Service Desk Agent	Service Desk Agents categorize tickets by choosing appropriate CCTI from the available categorizations in the Categorization lookup. Categorizing a ticket enables effective routing of the ticket, as well as facilitates in effective search for related solutions in the Knowledge Base .
Application Administrator	Application Administrator configures categorization for tickets by specify Class, Category, Type and, Item level categorization for different tickets as appropriate to the request type. The administrator sets up CCTI to be a matching condition for ticket Auto-Routes and workflow actions. The administrator also determines whether Self-Service Users can view and update the Type field to categorize tickets and controls the Types visible in the SSU ticket forms.

Ticket Assignment

Ticket Assignment is needed to ensure that the ticket gets owned by a specific individual, who then takes responsibility of closing the ticket.

Features	Ticket Assignment

Self-Service User	Self-Service Users are not involved in ticket assignment. Tickets logged by the Self-Service User gets assigned as per an Auto-Route that got applied. Self-Service users can view some details of the person who is currently assigned to work on a ticket they've logged.
Service Desk Agent	Service Desk Agents accept assignment of ticket in their support group queue. They can also manually assign a ticket to another support group or reassign the ticket within their group for action on the ticket.
Application Administrator	Application Administrator enables effective auto-assignment of tickets to appropriate Support Groups. This is done by allocating default assignment groups as well as configuring auto-routes to get applied on specific matching conditions. The Administrator also enables action options for manual assignment of tickets.

Ticket Updates

Ticket updates can be manual and automatic updates on actions taken on a ticket. This provides information on what has been done on a given ticket.

Features	Ticket Updates
Self-Service User	Self-Service Users can update tickets by adding a Worklog to the ticket from the Self-Service User Interface. They can also update a ticket by responding to email notifications from the ticket, which then gets appended to the Activity tab of the ticket.
Service Desk Agent	Service Desk Agents can update tickets by adding all required information to an open request, and by adding Worklog to the ticket. They can add worklogs, classify the Worklog based on worklog type and track time spent on the ticket. The ticket Communication Activity gets automatically updated on the ticket when Agents send out Notification or communication from the ticket. They can also update the ticket by responding to email notifications from the ticket.
Application Administrator	Application Administrator ensure appropriate ticket updates by Service Desk Agents by making the Worklog and time tracking as required fields; and by enabling the ability to send worklog communications as emails. They also allow communication from the ticket by enabling Send Mail option and providing communication templates to be used for communications.

SLA Compliance on Tickets

Processing of Service Desk tickets can be monitored for compliance with agreed upon Service Level Agreements. This helps better manage service delivery.

Features	SLA Compliance
Self-Service User	Self-Service Users are not directly involved in ensuring SLA compliance, but they can be notified if SLA targets are breached (depending on the company processes or policies).

Service Desk Agent	Service Desk Agents can see whether SLA compliance is applied to the ticket or not, and if SLA monitoring is enabled, they can see the Service Targets that have been applied to the ticket, Status of a Service Target (whether it is met, missed, approaching etc), and can prioritize their tasks accordingly. They can also add a note to indicate why a Target threshold was missed.
Application Administrator	Application Administrator can take actions to enable or disable SLA monitoring on tickets. If SLA monitoring is enabled, the Application Administrator configures the Service Targets against available Service Metrics, sets the threshold rules and actions to be taken in SLA target is missed.

Ticket Workflows

Ticket workflows control the movement of tickets from one status or phase to another; ultimately progressing towards ticket resolutions and closure.

Features	Ticket Workflows
Self-Service User	Self-Service Users do not participate in the ticket Workflow in terms of progressing a ticket towards Resolution . They log tickets, and respond to tickets, if required, to enable progression of the ticket by Service Desk Agents .
Service Desk Agent	Service Desk Agents move a ticket along its Workflow by taking different actions on the ticket at different stages of the ticket life-cycle. Their actions on the ticket are bound by the workflow configurations, and they can choose an action from among the available Action Options to progress the ticket towards resolution or closure.
Application Administrator	Application Administrator configures the auto-routes and Workflows based on the ticket progression and closure process identified for a given ticket type. The Auto-Routes and workflow configurations and the associated action options ensure that the ticket is progressed through the workflow as appropriate.

Related Tickets

Relating tickets to other tickets allows identifying a large issue and allows for identification of a problem, if any. Relating tickets also enables effectively working on all related tickets.

Features	Related Tickets
Self-Service User	Self-Service Users do not relate tickets to other tickets. This functionality does not apply directly to Self-Service Users .
Service Desk Agent	Service Desk Agents can establish Ticket Relationships by creating a new ticket as a Child of an existing ticket (if one ticket has led to the logging of the other) or relating tickets based on other criteria. Relating tickets enables identifying and collating details on all issues which may have a similar cause, similar impact or similar Resolution to be attempted. All related tickets can be seen on the Relate Tickets Tab.

Application Administrator	Application Administrator enables ticket relation as Parent Child relation by configuring Workflow action allowing creation of Child Tickets . They also take decisions as to whether an open ticket can be related to a closed ticket. Administrator can unrelate tickets related by Service Desk Agents.

Global Ticket

A Global Ticket is one that has far reaching implications, and impacts more than one individual issue. Marking a ticket as global allows it to be addressed effectively.

Features	Global Ticket
Self-Service User	Self-Service Users do not access the global ticket functionality, and they are not affected by this functionality.
Service Desk Agent	Service Desk Agents can mark a ticket as Global Issue ; and relate other issues to the global issue. This enables translation of action on the Global Issue to related tickets. Service Desk Agents can search for issues marked as global and manage related tickets accordingly.
Application Administrator	Application Administrator enables ability to mark a ticket as Global Ticket by enabling this action on the Ticket Toolbar . The administrator can also set a Special Function that will check for open tasks related to a Global Issue , to ensure that all related tickets are closed when a Global Issue is closed.

Related Configuration Items

As tickets could often be logged related to available Configuration Items , relating a ticket to a CI enables effective identification of potential problem areas and effective Resolution identification.

Features	Related Configuration Items
Self-Service User	Self-Service Users can relate a Configuration Item to a ticket, if the issue being reported is related to an available configuration item. A Self-Service User has limited ability to do this because he/she can relate only those Configuration Items that are related to him/her.
Service Desk Agent	Service Desk Agents can relate one or more Configuration Items to a ticket. They can view related CI records to identify where an issue exists and work on the ticket accordingly. The Service Desk Agent can also relate an Affected Service to a ticket, if the issue is being logged for a service.
Application Administrator	The application administrator manages the ability of Self-Service Users to view and relate Configuration Items to a ticket. The administrator can unrelate a Configuration Item related to the ticket by an agent.

Service Level Management

Service Level Management enables quantitative, time based measurement of response to tickets.

Feature Details	Service Level Management
Self-Service User	Self-Service Users are generally not part of the SLA escalation, management and monitoring process. This functionality is used mostly to measure performance of user request against pre-determined Service Level Agreement .
Service Desk Agent	Service Desk Agents ' working on a ticket can be monitored for various Service Metrics like Response time, Resolution Time, Ticket Closure time, etc. Service Desk Agents can view whether an SLA target is being applied to a ticket they are working on, pace their work on the ticket to be compliant with SLA targets, and add a note if needed about an Service Level Agreement target.
Application Administrator	The Application Administrator determines whether Service Level Agreement monitoring functionality is to be enabled for their organization or not. The Administrator set up Service Targets against available Service Metrics , determines the threshold rules, action to be taken on violation, etc. All aspects of Service Level Agreement monitoring, related Notifications and actions are determined by the Application Administrator.

Approvals

Approvals ensures that a change ticket is completely thought through, reviewed and authorized before implementation.

Features	Approvals
Self-Service User	Self-Service Users could be Approvers or Reviewers of a ticket. A ticket would be submitted to them for approval or review before a change can be initiated.
Service Desk Agent	Service Desk Agents submit the ticket for Approval or Review. They can choose approvers or reviewers for a change ticket based on configurations, and submit the ticket for Approval or Review. The Service Desk Agent may need to provide additional information if requested by the approver or reviewer.
Application Administrator	Application Administrator configures Approval Groups for different ticket types, and associates the approval or review groups with the ticket action. They also control actions such as action on Approval or rejection, to enable multi-level approval for a change ticket.

Search Solutions

Knowledge Base Article can be used to find solutions to open tickets and use available knowledge to troubleshoot issues.

Features	Search Solutions
Self-Service User	Self-Service Users can search for solutions in the Knowledge Base from available Knowledge Base Article . This could reduce their dependency on support.
Service Desk Agent	Service Desk Agents can search for solutions to open tickets and view related Knowledge Base Articles. If appropriate, they can use the solution to resolve the issue and update the cause- Resolution field of the open ticket. Service Desk

	Agents may also be able to use recently resolved tickets to solve open issues.
Application Administrator	Application Administrator controls the ability of Self-Service Users and Agents to view a Knowledge Base Article , and allows or controls Service Desk Agents ' ability to use Recently Resolved Tickets in solving an open ticket.

Majority of the Ticket Related functionality is configurable by the application administrator and is managed via permissions . Permissions can be assigned to either individual Contacts, Support Groups, or Roles.

Non-Ticket Functionality

The tables below identify the key functionality offered by Nimsoft Service Desk and how Non-Ticket Functionalities are made available to Self-Service Users, Service Desk Agents and Application Administrator.

Email Based Working

The ability of Nimsoft Service Desk to send and receive Emails and work on them according to defined configurations enables users to access ticketing functionality via emails.

Features	Email Based Working
Self-Service User	Self-Service Users can log new tickets via emails to the support ID. This will automatically log a new ticket in the application. SSU can also update tickets by responding to Notifications received via email; and take actions such as submitting Approval or Service Feedback Surveys via email. Replies to email Notifications get related to the existing ticket from which the mail was sent. They can send additional information as email Attachments, which get related as Attachments to the ticket.
Service Desk Agent	Service Desk Agents can also log new tickets and add updates to tickets that they are working on via emails. They can send out communication and Worklogs to chosen recipients via email. Service Desk Agents, who are approvers, can also send Approvals via email. Service Desk Agents who are part of the Service Feedback Process can respond to a Service Feedback Survey via email.
Application Administrator	Application Administrator enables effective Email Based Working by configuring Auto-Routes for tickets logged via emails; defining workflow action for tickets logged via email; and enabling email based communication to identified stakeholders on different actions on a ticket. The also configure the email functionality for their slice and set parameters to control aspects like Attachment size, formatting of email responses etc.

Direct URL Links

Nimsoft Service Desk allows registered users to access the application via Direct UR Links embedded in email communication from the application.

Features	Direct URL links
Self-Service User	SSU can use the Direct URL links embedded in emails sent by the application to avoid the login process and directly access a particular page in the application. Direct URL Links can be part of Approval Notifications, Service Feedback Notification, etc.
Service Desk Agent	Service Desk Agents can use the Direct URL links embedded in emails sent by the application to avoid the login process and directly access a particular page in the application. Direct URL Links can be part of Approval Notifications, Service Feedback Notification, etc.
Application Administrator	Application Administrator can generate the Direct UR Links, with the required Authorization Token, and make them available to intended recipients via email Notifications for Approval and Service Feedback Surveys. System defined communication templates can be used for generating such communication.

Notifications

Nimsoft Service Desk can be configured to send out Notification on a range of ticket and non-ticket activities. These automated notifications enable users to keep updated about ticket progress as well as be informed of actions they are required to take.

Features	Notifications
Self-Service User	Self-Service Users are usually recipients of notifications from the application. This could include notification on action on tickets logged by the SSU, outstanding approval notification or notification on SLA related information or Service Feedback related notification.
Service Desk Agent	Service Desk Agents receive notifications regarding ticket assignment, actions on tickets, and other actions like ticket approval status, etc. The actions agents take on tickets could trigger notification to Self-Service Users or other stakeholders. They can also send manual communications from a ticket notifying the recipient about an action on the ticket, or requesting information from the recipient.
Application Administrator	Application Administrator enables automatic notifications to be sent on action on tickets. Attaching communication templates to workflow actions, Auto-Routes, Approval, service feedback surveys, password changes, etc. enables Nimsoft Service Desk to send out automatic notifications on various actions using the application. Notifications for processes such as Change Approval have their coded notifications, where additional administrative setup is not needed.

Out of Office Flag

All users can set an Out of Office flag; and designate a Deputy /Alternate contact for responding to Notifications when they are out of office.

Features	Out of Office Flag
Self-Service User	Self-Service Users can set an Out of Office flag and nominate a Deputy to respond to Notifications when they are away. They can choose a deputy from among visible contacts if a default deputy is not already set.
Service Desk Agent	Service Desk Agents can set an Out of Office flag and nominate a Deputy to act on their behalf when they are away, in the same way as Self-Service Users access this functionality. They may see a Deputy contact has submitted an Approval on behalf of an identified Approver.
Application Administrator	The application administrator controls Out of Office functionality in two ways. One is by designating a default deputy for a contact in the Contact Records. The second is by identifying communications from chosen templates, which should not be diverted to the deputy even when the Out of Office flag is set. This ensures that only those communications that need immediate action get diverted; and select communication is not diverted to a Deputy.

Global Search

All users can access Global Search functionality from across all forms or sections of the application. Based on permissions granted, and the status of a record, Global Search displays records matching the search query.

Features	Global Search
Self-Service User	Self-Service Users use Global Search to search for records that are available to them. This includes searching for tickets logged by the SSU as Requester (or others in the SSU organization) and Knowledge Base Article.
Service Desk Agent	Service Desk Agents access a wider scope of search using Global Search. They can search for Tickets, Configuration Items, Knowledge Base Article, Contacts, Support Groups and Organization related records.
Application Administrator	Application administrators access Global Search in the same way as Service Desk Agents do. As Administrators have access to a wider range of records, their search results will produce more records than through search by Agents.

Advanced Search

Advanced search allows users to define their own search, filtering the search using one or more factors. Depending on the user type, the availability of Advanced Search feature differs greatly.

Features	Advanced Search

Self-Service User	Self-Service Users can use advanced for Tickets; wherein they can search for tickets by Ticket ID, Priority, Type, Status, or Date Range. SSU cannot search for any other record like solutions using Advanced Search.
Service Desk Agent	Service Desk Agents can access a range of Advanced Search for ticket and non-ticket records. They can access Advanced Search to search tickets from across all ticket modules, for a ticket within a ticket module or to search for Configuration Items. An advanced search type functionality is also available when attempting to Relate Tickets from within the Relate Tickets tab.
Application Administrator	Application Administrator can access Advanced Search in the same way as Service Desk Agents. They do not make any configurations or control Advanced Search feature in any way for Agents or Self-Service Users.

Defined Search

Advanced search allows users to define their own search, filtering the search using one or more factors. Depending on the user type, the availability of Advanced Search feature differs greatly.

Features	Defined Search
Self-Service User	Self-Service Users can use advanced for Tickets; wherein they can search for tickets by Ticket ID, Priority, Type, Status, or Date Range. SSU cannot search for any other record like solutions using Advanced Search.
Service Desk Agent	Service Desk Agents can access a range of Advanced Search for ticket and non-ticket records. They can access Advanced Search to search tickets from across all ticket modules, for a ticket within a ticket module or to search for Configuration Items. An advanced search type functionality is also available when attempting to Relate Tickets from within the Relate Tickets tab.
Application Administrator	Application Administrator can access Advanced Search in the same way as Service Desk Agents. They do not make any configurations or control Advanced Search feature in any way for Agents or Self-Service Users.

Personal Search

Ability for users to choose the language in which the UI is available to them, by setting their own locale preference. Administrators can define a default locale for all customers

Features	Personal Search
Self-Service User	This feature is not available for Self-Service Users, as the requirement for Self-Service Users to search for records is very limited.

Service Desk Agent	Service Desk Agents can configure their own Personal Search for Ticket and CI records by specifying their own Display List and Search Criteria. These searches can be created, modified or deleted by the Service Desk Agents on their own with no assistance needed from the application administrator.
Application Administrator	Application Administrator can create new Personal Searches for Tickets and CI records, similar to Service Desk Agents. They however, do not play a role in configuring personal searches for other contacts or support groups, nor do they control access to these records that are created by the logged in Agent user.

Reports

Nimsoft Service Desk provides a range of out-of-the-box reports related to Tickets, Configuration Items, Knowledge Base Article, and Service Feedback Surveys. Reports can be seen within available link within each module; or in the Trends and Metrics Module of Nimsoft Service Desk.

Features	Reports
Self-Service User	Self-Service Users do not have direct access to any reports. This functionality is not available on the Self-Service User Interface.
Service Desk Agent	Service Desk Agents can view and access a range of reports related to Tickets, Configuration Items, Knowledge Base Articles, and Service Feedback Surveys depending on whether they have been given access to view and generate a specific group of reports related to a module. They can view and generate only those reports, within a module, to which they have been granted permission.
Application Administrator	Application Administrator can access a range of out-of-the-box reports related to different ticket and non-ticket modules. They control the ability of Service Desk Agents (Support Groups , roles, or individual contacts) to view Reports link and a set of related reports within each module as well as the ability to view the Trends and Metrics Module. The administrator controls the access to reports via permissions.

Dashboards and Charts

A user logged into Nimsoft Service Desk can view Dashboards and Charts depicting the status or progress of their tickets against different parameters.

Features	Dashboards and Charts
Self-Service User	Self-Service Users have very limited access to Dashboards and charts. Their access is limited the chart that they see on the Home Page, which displays the Status of Tickets logged in the past 30 days.
Service Desk Agent	Service Desk Agents have some control on the charts and dashboards available to them. They view three charts on their List Tickets Page, and they can choose

	alternative charts from the options made available to them under Home>Update My Preferences. Also, they can access a My Dashboards page if access is permitted by the administrator. This lets them view different Dashboards , and set a dashboard page as Home Page.
Application Administrator	The Application Administrator manages the ability of Service Desk Agents to view and access Dashboard Charts and access the My Dashboards link. The administrator can configure new Charts and make them available for use in a dashboard; and manage Permissions to access these charts via the permissions tab. The administrator can also configure Dashboards and make them available to users or Support Groups

Knowledge Base Articles

Users can access Knowledge Base Articles relevant to them; and use the solutions from the Knowledge Base to resolve their own queries.

Features	Knowledge Base Articles
Self-Service User	Self Service Users can view those Knowledge Base article that they have been granted Permissions to view. They can search for articles from the Knowledge Base link or search for articles using Global Search . Self-Services Users can view the average rating of a Knowledge Article , comment on the usefulness of a Knowledge Article , provide feedback about it, and give the article a rating. They can view attachments related to a Knowledge Article to gather more relevant information.
Service Desk Agent	Service Desk Agents can Add articles to the Knowledge Base and view Knowledge Base Articles when searching for relevant articles either from a ticket or from the Knowledge Management Module. They can also comment on the usefulness of a Knowledge Article , provide feedback about the article, and submit a rating for the article. Service Desk Agents can also view feedback and comments by other users and contacts on how frequently an article was viewed and how often it solved a user issue. They can also relate an attachment to an article; or view an attachment related to the article.
Application Administrator	The Application Administrator reviews all new additions to the Knowledge Base; and sets the status of the article to Approved for the article to be usable for other users. The administrator can also relate an article to a Configuration item, CCTI of a CI, or an Organization ; upload an attachment to the article and add key words manually. The administrator manages permissions for Self-Service Users and Service Desk Agents to view a Knowledge Article via the permissions tab. The administrator also determines access to the Knowledge Management link for Self-Service Users and the maximum number of records to be displayed in a Solutions Search.

Service Feedback Surveys

Service Feedback Surveys are qualitative means of measuring performance of the IT Support team.

Feature Details	Service Feedback Surveys
Self-Service User	Self-Service Users respond to Service Feedback Surveys based on schedules established by the Application Administrator . They can respond to the Survey either from the link available in the application or via the link embedded in the email Notification for a Survey.
Service Desk Agent	If Service Desk Agents are made part of the Service Feedback process, they can participate in the Service Feedback Surveys in the same way as Self-Service Users. Depending on the support group type or role, some agents may receive and review Service Feedback responses and view related reports.
Application Administrator	The Application Administrator create Service Feedback Surveys and set a schedule for the Surveys to be sent to identified contacts and Support Groups. The administrator can configure a list of surveys as per organizational need. Service Feedback Surveys can be configured for multiple choice responses or single line or multi-line text responses. You can also configure Service Feedback to solicit Anonymous Feedback without reference to the respondent or send it to specified respondents. You can also specify schedule repetition patterns.

Attachments

Attachments can be used to give additional information to a ticket, besides what is captured in the ticket fields. Attachments can also be related to other records like Knowledge Articles, Configuration Items, Contact and Organization

Features	Attachments
Self-Service User	Self-Service Users can relate an attachment (of a set maximum size) to a ticket they have logged. This attachment gets related to the ticket that is created based on the email and can be viewed from the ticket form.
Service Desk Agent	Service Desk Agents can relate multiple Attachments to the ticket, if required. They can mark an attachment as Global Attachment, to make the attachment available to other users for other tickets and other records which allow for attachments. Agents can also relate attachments and view attachments related to Knowledge Articles, Configuration Items, Contact and Organization records.
Application Administrator	Application Administrator determines the maximum allowed attachment size, and also controls very small files like email attachments containing sender signature title etc. from getting attached to tickets. The administrator can unrelate an attachment related by an Agent or self-service user to a ticket and relate or unrelate attachments from Organization, Contact, Configuration Item and Knowledge Articles as required.

Data Exports

Data from the application can be extracted in the form of PDF or CSV files; and physical prints.

Features	Data Exports
Self-Service User	Self-Service Users can export data on ticket lists and ticket search results into PDF or CSV files. They can also print a ticket for their records.
Service Desk Agent	Service Desk Agents can export data on Ticket Lists, Configuration Items list, Knowledge Articles list, and search results into PDF or CSV files. They can also print tickets for future records or reference.
Application Administrator	Application Administrator access the data extract functionality in the same way as Self-Service Users and Agents. They do not impose any additional restrictions on this functionality.

Filter for Lists

Users can use filters to restrict what they view in the lists. These filters could be set for that session; or be saved as preferences by individual users.

Features	Filter for Lists
Self-Service User	Self-Service Users see only limited entries in the ticket lists and other lists on the SSU interface. They therefore do not have access to filters for lists. If a Self-Service User has access to view My Organization Tickets, he/she can filter the list to either view their own requests or requests for their organization.
Service Desk Agent	Service Desk Agents can use a range of filters across all ticket modules and non-ticket modules. They can use filters available on the form page to set filters for that specific session; or they can select preferred filters which will remain in effect till the filters are reset to default.
Application Administrator	Application Administrators can use filters in all ticket modules, non-ticket modules as well as the Administrative forms. For example, they can filter records for Status (active or inactive) or for system-defined records. They can choose filters based on the need of the action they are performing to contract or expand the lists visible to them.

Locale Preference

Users can select their own locale preference and thereby control the language in which the UI is available to them

Features	Filter for Lists
Self-Service User	Self-Service Users can select their own locale from the Self-Service User Interface, and set a Locale preference different from the System Default locale.
Service Desk Agent	Service Desk Agents can select their own locale from the Application Interface, and set a Locale preference different from the System Default locale. If they are involved in configuring a Contact record, they can also set the locale preference for the newly configured contact.
Application Administrator	Application Administrator defines the System Default locale that will be applied by default to all contacts of that slice, if no preference is selected by the logged in user. To make other custom defined entities like Custom Fields, Workflow Action Options etc in a different language, the Application Administrator has to configure these entities in English and provide translation for each entity in other available languages.

Other functionality such as Bulk Process of Data, search for communication history, schedule logs, etc. are available exclusively for the application administrator.

Frequently Asked Questions

As Administrators, you may have many questions related to Nimsoft Service Desk. You may also have questions on configuring the various features of the application. This section lists generic questions that administrators of Nimsoft Service Desk could have while using the product.

Given below is a list of FAQs related to Generic Queries.

How is the first administrator for an instance of the application created?

The first administrator for your instance is created during the Slice Provisioning stage. During Slice Provisioning, the Super Administrator configures the first administrator, who can then log into the application instance and configure all other records.

Is the first Administrator the Super Administrator for that slice?

No, the first administrator is a contact who has default administrative rights for your instance of the application. The Super Administrator is a role performed by Nimsoft Service Desk Support Team and is responsible for managing all customer slices (tenants) and assisting the customer application administrator of each individual slice.

What are the default permissions granted to the First administrator?

The first administrator has default access to all features and functions of the application. The first administrator can perform all tasks required for configuring and managing your instance of the application.

Does the First administrator have any extra privileges compared to other additional administrators created?

No; all administrators have access to every action, feature and functionality of the application. There is no difference in permissions or privileges assigned to the first administrator and any other administrator added later on.

How many Administrators can one slice of Nimsoft Service Desk have?

There is no upper limit on the number of administrators for one slice of Nimsoft Service Desk. However; to avoid confusions and minimize chances of an action by one administrator overriding actions by another; it is advisable to limit the number of members in the Administration Group.

Who can create additional administrator(s) and assign permissions to them?

The first administrator can create other contacts and make them member of the Administration group. Once made part of this support group as Primary Group, these contacts get default administrative permissions and privileges.

Can I assign permissions for only some modules to be managed by one administrator?

If a contact is set as Administrator in system created Administrator group, by default all permissions to access and manage all sections of the application become available to the contact. You cannot assign administrative permissions per module.

As a workaround, you can create a Support Group with an appropriate name (Except Administrator), and assign access to specific forms and navigation menu links (like Manage Contact or Service Feedback) to the contacts related to that support group. The members of this group will have Administrative privileges to those forms and actions that they have permission for.

Can one administrator revoke permissions granted to another administrator?

Yes; by removing a contact from the Administrator group and assigning only limited permissions for the contact as if he/she was an agent, one administrator can revoke permissions granted to another administrator.

What are the actions or transactions that can be managed by email? Do I need to make special configurations for these?

Nimsoft Service Desk enables email based logging of tickets, email notification for actions and updates on tickets, manual email communication from tickets, worklog updates via email, and email notification for activities like ticket assignment, approval notification, and service feedback notification.

You will need to configure the support email id for tickets to be logged in response to emails to that id. You can also configure auto-routes for the tickets based on email Subject and configure multiple email ids for one instance.

The configuration of email id(s) for your slice is currently taken up by the Super Administrator.

Chapter 4: Access and Permission

Overview

Permissions relates to the ability of a contact to access the application or a record within the application. Permissions to a record can be assigned either to an individual contact, or a contact can inherit permissions by virtue of being related to a Support Group or Role.

As Application Administrator, you can manage the ability of a user to interact with the application by controlling a logged in user's access to specific record/record types.

The ability of a contact to interact with the application can be controlled in three ways:

1. By managing access to the application by enabling login and by assigning an appropriate license type for a contact or end user.
2. By managing access to specific records like Knowledge Articles, Workflow Actions etc. by enabling or disabling Permissions to an individual record/record type.
3. By managing access to ticket and CI records by virtue of relationship of the contact with an Organization record within the application instance.

By enabling login and assigning an appropriate license type (Self-Service, Fixed, Floater or Web Service), you can control what a logged in user is able to access, and control the actions the user can perform.

Permission to access records like Knowledge Articles, Ticket Templates, Workflow Actions etc., can be managed by enabling permissions to each individual record to a Contact/Support Group/Role.

Access to a Ticket, Configuration Item, Contact and Support Group records can be controlled by enabling Organization based Security and relating a Contact or Support Group to an organization.

All aspects of access and permissions that are managed by the Application Administrator are explained in this section.

Manage Access

As application administrator, you can manage the ability of contacts to access the application.

To be able to access Nimsoft Service Desk, a contact has to have a system login with appropriate License Type and the Status of the contact has to be Active .

The other aspects that control the ability of a contact to interact with the application are explained below.

Licenses

The primary means of controlling access permitted to a contact is by enabling system login and providing the contact an appropriate license type.

If a contact does not need to interact directly with Nimsoft Service Desk in any capacity, you can choose not to Enable System Login for that contact. No Login credentials will be created for this contact record, and the contact will not be able to access the application.

A contact whose system login is enabled, will need to be given an appropriate License Type to access the application.

Next, you can assign a contact either a Fixed License , a Floater License or a Self-Service User License. You could also choose to associate a contact with a Web-Services License to interact with Nimsoft Service Desk via web services.

A contact can be given only one kind of license at a time. However, to accommodate any changed need, you can change the License Type assigned to a contact at a later stage.

The screenshot shows the 'Contact Profile' form in Nimsoft Service Desk. Key elements include:

- Contact Details:** Fields for Title, First Name, Middle Name, Last Name, Email, Job Title, Department, Office/Cube, Pin #, Time Zone, and Deputy/Alternate.
- Status:** A dropdown menu set to 'Active'.
- Access Enabled:** Checkboxes for 'Enable Login' (checked) and 'Out of Office'.
- License Type:** Radio buttons for 'Self-service', 'Fixed', 'Floater', and 'Web Services'. 'Self-service' is selected.
- Reset Password:** A button to reset the contact's password.
- Support Group:** A table with columns 'Support Group' and 'Primary Group'. The row shows 'BesTSM Baroda L1' as the primary group.

A contact who has been given Self-Service License automatically gets associated with the Self-Service Group as primary group ; and the contact gets access to the Self-Service User interface of the application.

Other contacts, with login enabled get access to the Agent/Admin Interface of Nimsoft Service Desk.

A contact assigned Web-Services license interacts with the application via the web services interface, but will not be able to access the application using the application User Interface.

Status of Entity

For a contact to be able to login and access Nimsoft Service Desk, the Status of the contact record has to be Active .

Even if the contact has login enabled and has a valid license associated, s/he will be unable to access the application if the Status of the contact record is set to inactive.

It is also possible to manage the status of an entity at the Organization, Site, or Location level.

When an organization status is set to inactive, all sites and locations related to that organization become inactive; and all contacts records, with the inactive organization as Primary Organization, also become inactive. Contacts related to an inactive site or inactive location also become inactive even if the Organization is still in Active Status.

Thus by controlling the status of an individual user's Primary Organization, Site or Location, you can control the access to the application.

Note: Please note that while you can set the Status of entities lower in the hierarchy to Inactive by making a higher level entity (like Organization/site/location or support group) inactive; you cannot make all related entities Active by setting a higher level entity Status as Active .

You have to manually set the status of all relevant entities as Active.

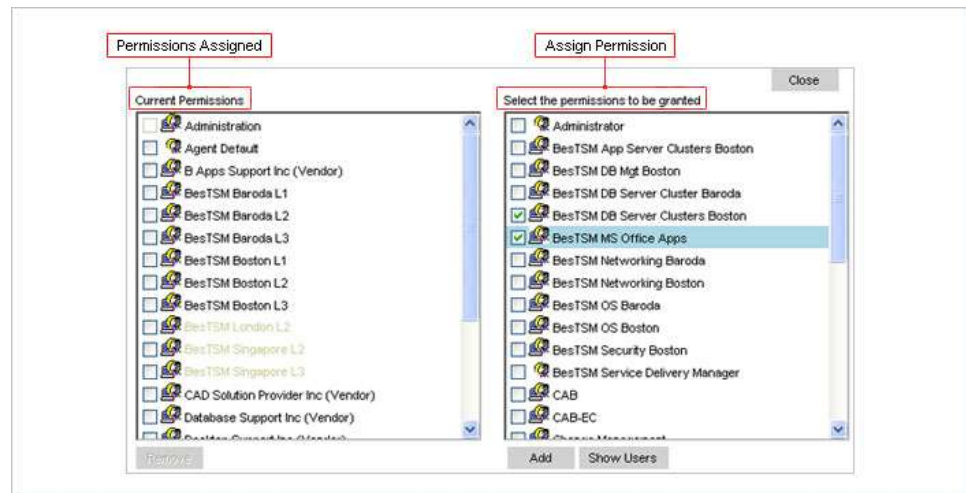
The table below represents how the relationship of a contact with an organization, and the status of each entity impacts the ability of the contact to log into the application.

Contact "Login Enabled"	Contact Status	Linked Organization	Able to Login
True	Active	Primary Organization Active	Yes
True	Active	Primary Organization Inactive	No
True	Active	No Primary Organization	Yes
True	Active	No Organization Linked	Yes
True	Inactive	NA	No
False	NA	NA	No

Manage Permissions

As Application Administrator, you can manage the ability of Self-Service Users or Service Desk Agents to access a specific feature or functionality of the application. Permissions can be granted or revoked at the individual contact level or via the support group or role, to all contacts related to that Support Group or role.

This section lists all areas where you can enable or disable access to a feature or functionality for different users or groups.



There are three pre-defined Support Groups based on license and user type:

- Self-Service Users (all contacts with license type as Self-Service)
- Public (all contacts with Fixed/Floater license)
- Administration (the first contact configured as administrator during Slice Provisioning)

These groups can be used for effectively managing permissions. You can also configure other Support Groups and Roles as per your needs. Permissions can be assigned to an individual contact (example in situations where a Contact is not related to any support group) or to a Support Group or Role. All contacts related to a Support Group/Role will inherit permissions assigned to the Group/Role.

Note: For all contacts with Self-Service License, by default the Primary Group is Self-Service. Even if the user is assigned additional permissions to Navigation Items and actions that cannot be accessed from the Self-Service Interface, the contact will not be able to view or perform the identified action.

Where permission is to be given to all contacts (from all support groups except Self-Service User Group); permission can be given to Public Group.

Where a contact is made member of Administration Group; by default access to all forms and records becomes available to the contact.

Navigation Menu

You can control the ability of users to access different sections in the Navigation Menu ; as well as individual links within a chosen section.

Depending on the role that a contact, support group or role plays with the IT Support structure, you can enable access to only those links and sections where the logged in user would be required to interact with Nimsoft Service Desk.

As application administrator, you can control the links that Self Service Users view in the Self-Service User Interface as well as links for actions enabled to Service Desk Agents.

For example, consider a Level 1 Support Groups which has to log all user requests, and forwards them to a Level 2 Group; and respond to customer queries on progress of their request.

Given this limited interaction with Nimsoft Service Desk, the Service Desk Agents associated with this Level 1 Support Group need access to functions like Logging Service Request , and Search for all Ticket types.

You can therefore enable access for this Support Groups to just the links under the Request Management Module and Search related links for other Ticket Modules.

The Level 2 Support Groups , which actually classifies the requests, and works the ticket through its life-cycle, could be given access to a larger suite of application features and functionality.

Similarly, for contacts who have the Role of a Support Supervisor or IT Manager; where they extensively use Dashboard or Reports, you could give access to links that enable them to view Dashboard or extract reports.

Thus, by allowing or limiting access to an item in the Navigation Menu, you can control the feature or functionality which a specific Role, Support Group or Contact accesses. By choosing permissions to access carefully; you can ensure that a contact has access to the application functionality that they really need; and use frequently.

Ticket Toolbar

Depending on the Workflow actions and activities that a Support Group or Role may be required to perform; you can limit the actions available to them on the Ticket Toolbar . Service Desk Agents can perform only those actions that they see on the ticket toolbar.

For example; if you do not wish to allow agents related to a Level 1 Support Group the ability to Add Solutions to the Knowledge Base ; you can disable the “Add to Knowledgebase” action.

By not enabling permissions to this action for the Level 1 Support Group, the “Add to Knowledgebase” can be hidden from that support group and contacts related to this group will be unable to take this action.

Thus by controlling access to action items on the Ticket Toolbar ; you can manage the actions that a given support group or role is allowed to take.

Reports

Nimsoft Service Desk enables you to access a range of out-of-the-box reports related to Tickets, Configuration Items , Knowledge Base Article and Service Feedback responses.

You can control access to these reports and enable access to Support Groups or roles based on their need to access and view these reports.

For example, the role of Service Delivery Manager would require access to various reports related to the performance of ticket, SLA compliance etc. and Service Feedback while the role of IT Infrastructure Manager would prefer reports related to Configuration Items , and Service Availability.

As Application Administrator , you can enable access to the Trends and Metrics Module to those Support Groups or Roles which need access to these reports. You can also enable access to specific reports for other Support Groups , depending on their need.

Dashboards and Charts:

Nimsoft Service Desk provides a range of out-of-the-box charts and dashboards related to Tickets and Configuration Management. As application administrator, you can also create new Charts and make these charts available to different users for configuring their own Dashboard .

You can enable access to dashboards for supervisors or support managers, who would benefit by the visual inputs provided by such Dashboard charts. You can control access to the dashboards and charts by enabling or disabling access to the My Dashboards link under Home.

Defined Searches

Nimsoft Service Desk provides a range of out-of-the-box defined searches to enable users to quickly search for records within a given module.

As the application administrator, you can configure new **Defined Searches** as per the search needs of different users, roles or **Support Groups** .

Depending on the type of searches that an individual or support group needs as part of their daily operations, you can enable permissions to a **Predefined Searches** query.

You can control the ability of **Service Desk Agents** of different groups to access the system-defined and non-system **Defined Searches** via permissions from the **Manage Defined Searches** link under **Application Setup**.

Workflow Actions

The progression of a ticket through its life cycle depends on the **Workflow** that are configured for a given ticket type. However, not all **Workflow** actions configured, are required by all support groups.

For example, you may want to limit access to a workflow action of **Assign Emergency Change for Implementation** to only those **Service Desk Agents** who are part of the **Change Management Group**.

As application administrator, you can control access to all workflow actions by assigning permissions to the **Workflow** action for a contact, support group or role. All existing **Workflow** actions have a **Permissions Tab**; through which you can control permissions to a workflow action.

Ticket Templates

Nimsoft Service Desk allows you to create various **Ticket Templates** for logging standard requests, incidents, problems or changes. You can also configure templates for **Task Groups** and **Task Flows** .

However, not all template that are created will be needed by all support groups or roles. For example, a **Level 1** support group, which is not required to submit **Task Tickets**; need not be given access to **Task Groups** or **Task Flows** .

As application administrator, you can enable or disable access to a ticket template, task group or **Task Flow** . All **Ticket Templates** have a **Permissions Tab** through which you can control access to the **Ticket Template**.

Communication Templates

Nimsoft Service Desk allows you to create **Communication Templates** which can be associated with manual and automatic **Notifications** from the application.

Like all other functions, Service Desk Agents, Support Groups and Roles need access to only those Communication Templates related to the functions that they access and use as part of their daily operations.

As Application Administrator, you can control the ability of Service Desk Agents to be able to access Communication Templates for manual Notifications from a ticket. You can enable or disable access to a Communication Template for a contact, support group or role.

All Communication Templates have a Permissions Tab through which you can manage permissions to the Communication Template.

Knowledge Base Articles

You can build a Knowledge Base in the Knowledge Management Module of Nimsoft Service Desk. The Knowledge Base Articles can include solutions to common incidents, informative articles, response to frequently asked questions and other such useful information.

You can manage the ability of Service Desk Agents and Self-Service Users to view and use these Knowledge Base Article via permissions.

As not all knowledge Articles are of use to all contacts, Support Groups or roles, you can limit the ability of a contact to access a Knowledge Article. All Knowledge Article have a Permissions tab through which you can control this access.

Organization Based Security

Organization Based Security means the ability to control access of transaction records to a logged in user based on the Organization that the logged in user is related to. You can enable Organization Based Security model as an additional feature, on top of the Permissions model for controlling access to records in the application.

Enabling Organization Based Security mainly impacts Agent/Analyst users' ability to view and interact with the related records. As the ability of Self-Service Users to interact with tickets is already restricted to only their own requests or requests for their Organization, the impact of enabling Organization Based Security is minimal for Self-Service Users.

Contacts with Administrator Privileges (contacts who are part of the Administration Support Group), will continue to be able to see all records as if Organization Based Security is not enabled.

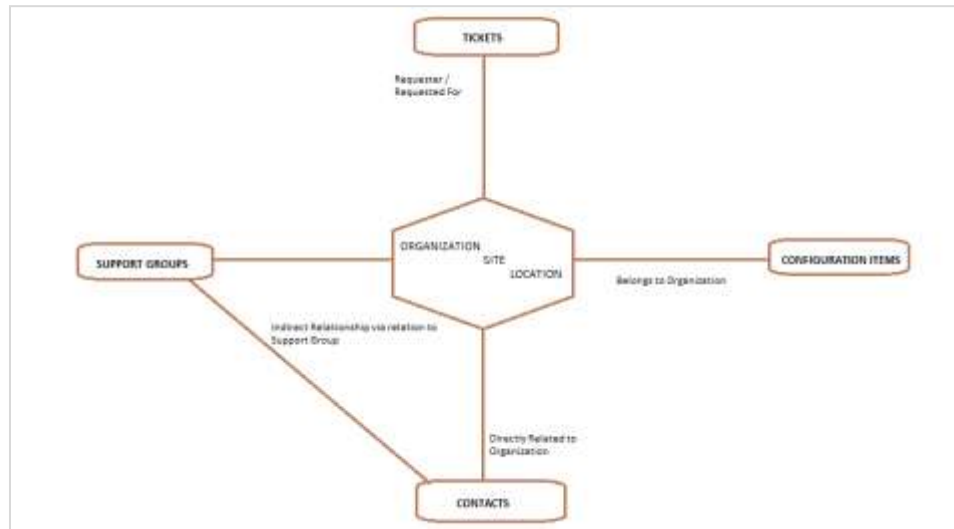
When Organization Based Security is enabled, a contact logged in as an Agent/Analyst, will be able to view only those Tickets, Configuration Items, Contacts and Support Groups, which are related to an Organization that they are directly or indirectly related to.

To enable Organization Based Security, you have to set the System Config Parameter `ENABLE_ORGANIZATION_BASED_ACCESS_CONTROL` to Yes.

Effective implementation of Organization Based Security is dependent of the following relationships between some entities in the application.

Relationship between Entities

Enabling Organization Based Security is based on relationship between Organization, Contacts, Support Groups, Tickets and Configuration Items.



The sections below explain these relationships further:

Organization-Contact-Support Group Relationship

The Organization-Contact relationship could either be direct; meaning the contact is directly related to the Organization; or could be inherited by virtue of the contact being related to Support Group(s) that are related to the Organization.

Note: A Contact/Support Group related to a Location (the lowest level of the Organization-Site-Location hierarchy), will be able to work only with Tickets and Configuration Items related to that Location. These Contacts/Support Groups will not be able to work with Tickets or Configuration Items related to the Organization or Site.

Organization- Configuration Item Relationship

Every Configuration Item is related to one Organization, and this relationship determines which Organization the Configuration Item belongs to. A configuration Item can be related to only ONE organization.

The Organization of the Owner of the CI (Contact related to the CI as Owner) does not imply any indirect relationship between the CI and the CI Owner's organization.

Organization-Ticket Relationship

When a ticket is logged, the Organization of the Requestor of the ticket and/or the Organization of the ticket Requested For become the Organization of the ticket.

The section below explains the implication of enabling Organization Based Security on the various aspects of user interaction with the application.

Implication on Tickets and Configuration Items

When a ticket is logged; the Requester's Organization and the Organization of Requested For become the ticket's Related Organization.

If the Requester and Requested for do not have a related Organization, the ticket has no related organization.

Thus, a ticket can be related to one, two or no organization.

The table below describes how Agents/Analysts interaction with tickets is impacted when Organization Based Security is enabled.

Action	Expected Behavior	Additional Information
Ticket Views	Ticket Lists will display only those tickets that belong to an Organization that the Agent/Analyst is related to. In the Related Tickets tab of a ticket, Agent/Analyst will be able to see only those related tickets that belong to Organizations that they are related to. Related tickets that belong to other organizations will be hidden. In the Related CI tab of the ticket, the Agent/Analyst will be able to view only those CI records that belong to related Organizations.	Ticket Lists for Default Assignment Groups will also list any ticket that has no related Organization. Note: It is recommended that Default Assignment Groups have at least one Administrator Contact so as to facilitate effective action on a Ticket with no Organization.
Ticket Creation	Agents/Analysts can log a ticket only on behalf of Contacts that are related to Organization(s) that they are related to. The name search lookup and filters will list only those contacts that meet the Organization relationship requirement.	If Agent/Analysts create a new contact record when logging a ticket for a Requester, they will be able to relate the contact only to an Organization they are related to.

Ticket Assignment	A ticket can only be assigned to Contacts/Support Groups related to the same organization as the ticket. The Assignment lookup lists only those Contacts/Support Groups belonging to related organizations. Note: For Ticket Assignment action, even Administrators will be able to see only Contacts/Support Groups related to the same organization as the ticket.	A ticket that has no related organization gets assigned to the Default Assignment Group as identified in the Default Assignment Group in Manage Config Parameters. Task Tickets get assigned to the Parent ticket's Default Assignment Group
Change Approvals	A Change Tickets that is submitted to a logged in user for Approval will be listed in the My Outstanding Approvals link only if the ticket belongs to an Organization that the logged in user is related to. This applies to Self-Service Users as well as Agent/Analysts. Note: When configuring the Change Approval process, Administrators must take due care to avoid situations where a Change Tickets gets assigned to a user who will not be able to view the ticket or act on it.	Change Approvers and Reviewers will be able to view Approvals and Comments by all other Approvers or Reviewers for the ticket; even if these comments are from Contacts who are not from the same Organization as the logged in user.
SLA Escalations	If a Ticket gets escalated to a Contact/ Support Group in response to an SLA Target violation; the Escalation action will fail if the Contact/Support Group is not related to the same Organization as the Ticket. Note: When configuring SLA Escalation Actions for a Service Target, due care must be taken to avoid escalation of a ticket to Contacts/Support Groups not related to the same Organization as the ticket.	If a ticket gets escalated by the SLA engine to a Contact/Support Group not belonging to a Related Organization, the ticket will get assigned to the Default Assignment Group

Ticket Searches	Ticket Searches will display only those tickets that belong to an Organization the Agent/Analyst is related to. This includes all types of searches including Defined Searches, Personal Searches, Advanced Searches and Global Search	For behavior related to Defined Searches, please refer to the section- Implication on Searches.
Ticket Activity Tab	The Ticket Activity Tab will display details of all actions on the ticket and communications (including manual and automatic notifications and worklogs) irrespective of whether it was entered by someone from a related organization or not.	The View Related option in the Activity tab will show the Activity Details only for those Related Tickets that belong to the same organization as the logged in user.
Affected Services on Tickets	If a ticket has an Affected Service related to it; it will continue to be visible on the ticket; even if the logged in user does not have access to the related Configuration Item. The logged in user will be able to change the Affected Service.	If the logged in user does not have access to the Affected Service, when attempting to view the Affected Service details a message "The Configuration Item you are requesting does not exist or you are not permitted to access it" will be displayed.

If an Agent/Analyst has access to the ticket but one of the contacts (either Requester or Requested for) does not belong to a related Organization; the contact details will continue to be displayed on the ticket, but the user will be unable to view the contact record of the contact. A message "The Contact you are requesting does not exist or you are not permitted to access it" will be displayed.

Administrators must take due care to ensure that Approvals and SLA Escalation Actions are configured correctly, so that tickets do not get assigned to Contacts/Support Groups that cannot access the ticket.

Implication on Email Communications

Enabling Organization Based Security could have some impact on the Outbound Email Communications from tickets and other records and actions from incoming Email Communications.

Some key implications for outgoing communications are listed below.

Action	Expected Behavior	Additional Information
Automatic Notifications from Tickets	Outbound Emails will be sent to recipients identified on the Communication Template used for the notification; irrespective of whether they belong to the ticket's related organization or not. However, when accessing a ticket using the Direct URL Link in the notification, if a user does not belong to a related organization, the user will be unable to access the ticket. A message "The ticket you are requesting does not exist or you are not permitted to access it" will be displayed.	Emails will get sent to a Support Group if the Support Group has an Email ID; even if the Support Group does not belong to a related organization.
Manual Notifications from Tickets	If an Agent/Analyst provide an email ID in the Send To field, (either using Send Mail or Worklog Send as Email), the notification will get sent to the recipient, irrespective of whether the recipient belongs to a related organization or not.	
Approval Notifications	If there is a mismatch between the recipient's organization and the ticket organization, the recipient will not receive notification for Feedback, Approvals etc.	
Action on Incoming Emails	An Incoming Email can result in the creation of a new ticket, to which an Auto-Route could get applied.	Auto-Routes will need to be reconfigured or appropriately modified to ensure routing of

	If the Auto-Route results in assignment of the ticket to a Contact/Support Group that does not belong to a related Organization; the Auto-Route will fail. The ticket will get assigned to a default assignment group.	tickets to a Support Group that can access the ticket.

Administrators must take due care when configuring the Send To, CC, BCC in a Communication Template to ensure notifications do not get sent to contacts who can't access the ticket. Also, Auto-Routes must be configured taking into account Organization-Contact-Support Group relationships.

Implication on Searches

When Organization Based Security is enabled, ticket searches will be affected and search results will display only those tickets belonging to the logged in user's organization.

Some other impacts on searches are listed below:

Action	Expected Behavior	Additional Information
Defined Searches	Defined Searches available Out of Box, (except ones with Negative ID) will not honor Org based Security even when its turn On. Depending on the nature of the Defined Search, the Search Query can be modified to enable restricting the search result for Organization Based Security.	An example of a modified query has been provided. Depending on the functionality, the query will need to be modified appropriately.
Personal Searches	Personal Searches configured by the logged in user for Tickets and Configuration Items will honor Organization Based Security.	
Search Communication History	If Agents/Analysts have access to the Search Communication History in Administrative Utilities, the Communication Records	Agents/Analysts will not be able to view non-ticket related communication records.

	visible to them will be limited. They will only be able to view Communication Records for tickets or related organizations.	

Below is a simple query change to enable Defined Search result to honor Organization Based Security:

```
SELECT <columns> FROM <table>[INNER JOIN <table having org Id>] WHERE <existing where clause> ${@eval.("${usercache.usergroup.is_user_an_administrator}".equals("false")) && "${sysliceconfig.enable_organization_based_access_control}".equalsIgnoreCase("true"))?( AND EXISTS ( SELECT 1 FROM vorg_contact_group_derived_relations WHERE slice=<outer table alias>.slice AND org_id =<outer table alias>.<outer table org id> AND user_id=${usercache.userprofile.user_id})):(){eval}
```

An example of a Defined Search modified using the above is:

```
SELECT row_id AS "ID", lvl1_name AS "Company Name", lvl2_name AS "Site Name", lvl3_name AS "Building", floor AS "Floor", suite AS "Suite", office_cube AS "Office/Cube", closet AS Closet FROM vorg_attrb_location v WITH(NOLOCK) WHERE slice=${usercache.userslice.active_slice} ${@eval.("${usercache.usergroup.is_user_an_administrator}".equals("false")) && "${sysliceconfig.enable_organization_based_access_control}".equalsIgnoreCase("true"))?( AND EXISTS ( SELECT 1 FROM vorg_contact_group_derived_relations WHERE slice=v.slice AND org_id = v.lvl1_id AND user_id=${usercache.userprofile.user_id})):(){eval}
```

Implication on Reports, Dashboards and Charts

When Organization Based Security is enabled, Reports, Dashboards and Charts will display results only for Tickets and Configuration Items belonging to the Logged in user's organization.

Some impacts on these aspects of the application are listed below.

Action	Expected Behavior	Additional Information
Ticket or CI related Reports	Reports for Tickets and Configuration Items will display results only for those records that belong to the Organization of the logged in User.	Reports based on Ticket and CI that have data Filters for Organization or Configuration Items or Service CIs , will

		have Look ups that list only the Organization / Configuration Items / Service CIs to which the logged in user has access based on Org based security model
Dashboards and Charts	Ticket and CI related Dashboards will display figures of records based on the Organization of the Logged in User.	

Data in the Dashboard Charts on the Home Page, and List page for each ticket type will be restricted by ticket data for the logged in user's related organization(s).

Implication on Knowledge Articles

While access to Knowledge Articles is not controlled by Organization Based Security (as it is managed by Permissions), there are some implications of related records on the Knowledge Article.

The Related Items tab of the KB Article will list only those Configuration Items and Organizations that belong to an Organization related to the logged in user.

Implication on Web Services

When Organization based Security is enabled, a Web Services User will be bound to viewing only those records that belong to related organizations. The Web Service user can be related to Organization, Site and Location; and will be governed by the same rules as applicable to other contacts with a Fixed license

The Web Service calls for Ticket and CI records will return only those records that belong to related Organizations as the Web Services user.

Implication on UMP Integration

The access to tickets via the My Tickets Portlet is affected when Organization Based Security is enabled.

When accessing the application via UMP, the My Tickets Portlet will display only those tickets which belong to Organizations that the logged in user is directly or indirectly related.

Implication on Configuring Records

Application Administrators can enable permissions to contacts that are not members of the Administration Group for actions such as Manage Contact, Manage Organization, Create CI etc.

When Organization Based Security is enabled, creation of such records by those who are not full Administrators (not members of Administration Group) will have several implications. These implications are explained below:

Action	Expected Behavior	Additional Information
Manage Organization	The Manage Organization List will display all Organizations irrespective of whether the Agent is related to that Organization or not. The Location Information tab will list all Sites and Locations, irrespective of whether the Agent is related to that Site or Location. The Contacts tab will list only those Contacts that belong to related organizations as the logged in user. When taking the Add Contacts action, the Name Search lookup will display only contacts from related organizations. The Groups lookup will display all Support Groups, irrespective of whether the Support Group is related to an organization related to the logged in user or not.	The logged in user will be able to create a new Organization Record with the only limitation being that the Add Contacts lookup will allow them to relate only contacts from related organizations.
Manage Support Group	The Manage Support Group list will display all Support Groups; irrespective of whether they belong to related organizations or not. The Location tab on the Support Group record will list only those Organizations that the logged in user is related to. When taking action to Add Location, the Group Location lookup will list only those Organizations that are related to	When an Organization is terminated, the Support Group remains intact; only relationship with the Organization is lost. This is irrespective of whether the Organization was related as Primary or not.

	the Logged in user. The Members list will display all contacts related to the Support Group. However, when Adding contacts, the Name Search Lookup will display only contacts belonging to related organizations.	
Manage Contacts	The Contact List will display only those Contacts that belong to related Organizations of the logged in user. A Contact can be related to multiple Organizations, the Location tab on the Contact Record will display only those Organization(s) that the logged in user is related to. When using the Add Location option to relate a Contact to an Organization, the lookup will list only those Organizations that the logged in user is related to. The Open Items tab and Related CI tab will display only those Tickets and Configuration Items that belong to related Organization of the logged in user.	When using Filter by Organization to view Contacts, the list will display only those organizations that the logged in user is related to.
Create Configuration Item	When creating Configuration Item records, there will be some limitations when relating Organization and contacts to the CI record. The Organization Lookup (to related Organization to the CI) will display only organizations related to the logged in user. The Name Search lookup for relating Owner for the CI record and relating other Contact/Support Groups to the CI record will display only Contacts and Support Groups related to the Organization.	If a Configuration Item is created by a contact who is not member of Administration Group, there could be implication on Organization and Contacts/Support Groups who can be related to the CI. This could have impact on Approvers/Reviewers associated with the Configuration Item.

The View Organization Tickets checkbox on the Support Groups record is functional only for Self-Service group. Checking it for other Support Group does not have any relation on enabling or disabling Organization Based Security.

The Support Groups tab on Organization records, and Location tab on Support Group forms will continue to be displayed, irrespective of whether Organization Based Security is enabled or not.

How Do I

Below are some actions you can take related to Managing Permissions.

Control access to various modules and links in the Navigation Menu

You can control the ability of users to access various modules and links in the Navigation Menu by assigning Permissions to Users, Support Groups, and Roles.

To Control access to various modules and links in the Navigation Menu:

Step 1: Click on the Manage Navigation Menus link under Administration Utilities. The List of Navigation Menus will be displayed.

Step 2: Click on a Navigation Menu item that you wish to modify access to.

The menu details will get displayed in the form below.

Step 3: Click on the Permissions tab of the record.

A list of users who have been granted permission to the link or module will be listed.

Step 4: Click on Manage Permission button to open the Permission Editor lookup.

Step 5: Choose names of contacts, support groups, or roles from the “Select the permissions to be granted” list and click Add.

The chosen names get displayed in the list under “Current Permission”.

Step 6: Choose names of contacts, support groups, or roles from the list under “Current Permission” by clicking the checkbox against their names and click Remove to disable permission to the selected contacts.

Step 7: Click Close to close the Permissions Editor.

A list of contacts, support groups and roles to whom Permission has been enabled will be displayed in the form.

By default Permissions for all actions and records is enabled for Administration Group; enabling all contacts who are part of Administration Group (with Fixed/Floater license) to access the full suite of actions and records. You cannot disable permissions for this Group.

Enable Organization Based Security

You can enable Organization Based Security to control access to Tickets and Configuration Items based on relationship of the logged in user to an Organization.

To enable Organization Based Security:

Step 1: Navigate to Manage Config Parameters in Application setup.

The Manage Config Parameter form is displayed.

Step 2: From the Parameter Category filter, select 'System'

Step 3: Click Refresh/Reload to apply the filter.

All Config Parameters related to System will be displayed.

Step 4: Select parameter 'ENABLE_ORGANIZATION_BASED_ACCESS_CONTROL'.

The Parameter details get displayed in the form below. The default value for this parameter is No.

Step 5: Set Parameter Value as 'Yes'

Step 6: Click Apply Changes.

Organization Based access control will now be enabled. Agents/Analysts' access to Tickets and Configuration Items, as well as Organization and Contact records will now be limited by related organization.

Note: Please review the implication of Organization Based Security on different actions before enabling this feature. You will reviews configurations like Approval Process, Auto-Route, SLA escalation actions etc. to prevent any potential conflicts.

Manage license assigned to a contact

You can provide an appropriate license type to contacts in Nimsoft Service Desk according to their roles and responsibility. To assign license to a newly configured Contact, the Application Tab gets displayed on the Contact record when the new contact record is configured. You can manage License assigned to the contact from this tab.

If you want to modify license issued to an existing contact record, access the Contact record from the Manage Contacts link under Application Setup.

To Manage License assigned to the contact:

Step 1: In the Contact record section, check on the Enable Login checkbox. This indicates that the contact will be able to log into the application.

Step 2: Click on the Application tab of the Contact record.

Step 3: Select a License Type based on the role that the contact will play in the application. You can choose only one license type for a contact.

You can choose between a Fixed, Floater, Self-Service User or Web-Services License.

Step 4: If a default System User ID is not configured, you can manually create a User ID in the System User ID field.

The contact will be sent out notification about the login ID and Password directly by the application.

If you run the Contact Synchronization to automatically sync users from your Directory server with Nimsoft Service Desk; all new users will automatically be assigned Self-Service User License; with the primary group set as Self-Service. You will need to modify the license for these contacts as appropriate.

You can set Email ID to become the default User ID for the contact by setting Slice Configuration DEFAULT_LOGIN_ID_TO_EMAIL_ADDRESS as yes.

View or Modify an Inactive Record in the Application

A new record that is created within the application is automatically set in an Active status. If the record is Deleted, the status gets set as Inactive. By default, administrative forms display only active records in the lists table. You can filter the list to view inactive records.

The steps below show how to view and modify an inactive workflow action.

Step 1: Click on the Manage Workflow Actions link under Workflow Tools.

By default, the list will display only Active records.

Step 2: Filter the list by Status in the Filter by section. The dropdown will display All, Active, and Inactive.

Choose to view only Inactive Records to view all Inactive workflow action option.

Step 3: Click on the Inactive Action Option that you wish to view or modify.

The details will get displayed in the form below. The status field will display the Status as Inactive.

Step 4: You can now modify the details of the Action Option to change any matching conditions or set fields as required.

Step 5: You can set the status as Active by selecting this option in the Status field dropdown.

Step 6: Click on Apply Changes. The changes will be saved in the record. If you have made the record active, the record will now become available for all relevant transactions in the application.

Some records like Organization, Contacts, etc. can also be permanently terminated. If a record is terminated; it will not be available to view and modify.

Frequently Asked Questions

Some questions that you may have regarding managing permissions or controlling access are listed below:

Can a user be given access to all functions and forms?

Yes; if you want to give a user permissions to all functions and forms across the application, assign the contact Fixed/Floater license, and make the contact a member of Administration Group.

All contacts related to the Administration Group will get default permissions to all forms and to all records configured in the application; and will be able to create, update or modify those forms and records.

Is there a way to enable permissions to all contacts designated as Service Desk Agents?

There is a pre-defined Support Group called 'Public'. All contacts (except those with Self-Service license) become default members of Public Group. If you assign permission to a record to this group, the permission is by default inherited by all contacts except Self-Service Users.

Can Agents access the reports visible in the Trends and Metrics Section?

Agents can access the Trends and Metrics section if you assign permission for access to this section from Manage Navigation Menu link under Administration Utilities. Further, they agent users (or relevant support groups) will be able to view those reports to which you grant access from Manage Report Configuration link under Administration Utilities.

The grouping of reports will be as per the grouping defined in the report configuration.

Do VIP Users have special permissions or access to some additional functionality?

No, VIP Users do not have any special permissions or access as these are controlled at contact, support group, or role level. Flagging a contact as VIP user is only a way of highlighting that the user requests need to be prioritized differently by the support group working on the request.

Can I assign permission access to reports to a Self-Service User?

While the application will not control your ability to assign permission for access to reports for Self-Service Group (the Self-Service Group will be displayed in the Permission Editor), Self-Service Users can view and access only those records that are accessible from the Self-Service User Interface. The Self-Service User Interface does not provide for access to any reports. Therefore; even if you assign permission to reports for a user assigned a Self-Service User license, the user will not be able to view or access the report.

Chapter 5: Internationalization

Overview

This sections presents information on implementation of Internationalization and Localization in Nimsoft Service Desk. This section provides an overview of the changes introduced to enable Internationalization, assumptions and intended behavior of the application in internationalized contexts as well as the known limitations related to Internationalization.

Leveraging the concept of locales, Nimsoft Service Desk offers the ability for customers and end users to use the application in other languages besides English. Currently, customers can choose from the available locale options of Chinese, English, Japanese, Portuguese, and Spanish.

Nimsoft Service Desk maintains language catalog at two different levels; one at the System level and one managed by the customer. The System level language catalog contains predefined translations for the supported languages. Items like Application Labels, messages and selected areas of the Quick Start data are part of the System language catalog and are available out-of-the-box for all customers.

In addition to this, customers can define their own translations for custom defined entities and records, like custom defined Attributes and Attribute values, workflow Action Option names etc. These items become part of the customized language catalog updated and maintained by the customers.

Approach

To facilitate end-user's ability to access the application in supported languages, items such as Field Labels, Action Links, Action Button legends, Tool Bar Names, Toolbar Items, Navigation group Names, Navigation Item Names, Filter Titles, Filter Drop Downs, and Messages are made available in the supported languages out of the box as bundles.

In addition to this, certain data from the Quick Start Configuration Guide will also be available as out of the box bundle. These are limited to the names of workflow entities/descriptions, ticket template names/descriptions, task group names, defined search names/descriptions. CCTI values, custom field labels, system defined metric names/description, ticket status, ticket reason code, ticket phase, ticket Priority, Urgency, Impact, CI status etc.

For Communication Templates available out-of-the-box, besides the Template Names/descriptions, the Subject and Body text will also be translated in the supported languages.

The main changes introduced to facilitate the ability of users to access Nimsoft Service Desk in other supported languages are explained below.

Setting User Locale

The following changes have been introduced to enable setting of locale preference for end users.

Slice Config Parameter

The following new Slice Config Parameters have been introduced for enabling Internationalization and Localization.

SYSTEM_DEFAULT_LOCALE:

This parameter is used to set the default locale on creation of new user contact through bulk upload process, AD Sync or where the user has to explicitly set a preferred locale.

ENABLE_SHARING_OF_LANGUAGE_TRANSLATIONS

This parameter can be set to Yes to enable customized translations for the slice to be shared with the Management slice. Only New Translations, updated after the parameter value is set to Yes, will be shared with the management slice.

ENABLE_KEYWORD_BASED_KB_SEARCH

This parameter can be used to turn on or turn off the Keyword based search for knowledge articles in the knowledgebase. Keyword based search can be replaced with a Java based Full-Text search by setting this parameter value to No.

If majority of the users are going to use knowledgebase search in language other than English, it is advisable to set this parameter value to No, and thereby enable full-text search. This is because Keyword based search is based on the Soundex algorithm, and therefore useful only for search for English text.

Self-Service User Interface

Self-Services Users can change their locale preference, and set a locale different from the slice default locale or locale set in their contact record.

The My Profile form under User Services in the Navigation Menu of the Self-Service User Interface has been changed to include a field for viewing and selecting the logged in user's preferred locale.

The field displays dropdown options showing the supported locales. The logged in user can select the preferred locale and click Update to set their preferred locale.

For the locale preference to take effect, the user will need to log off and log back in to the application. The UI and all system defined fields become available in the selected language. If you have made translations for items like Request Templates, FAQs etc., these will also be displayed in the selected language.

Agent and Administrator User Interface

Agent/Analyst users and Administrator(s) can also set their own locale preference as logged in users.

The Update My Profile form Under Home in the Navigation Menu of the Agent and Administrator interface has been modified to include the field of locale for viewing and selecting the logged in user's preferred locale. The field displays options showing the supported locales.

The logged in user can select the preferred locale and can click Apply Changes to set their preferred locale.

The Language and Date Format field get updated based on the locale selected.

For the locale preference to take effect, the user will need to log off and log back in to the application. The UI and all system defined fields become available in the selected language. If you have made translations for items like Request Templates, FAQs etc., these will also be displayed in the selected language.

Note: If any locale other than English or Default is selected, the Browser preference automatically switches to Cross Browser mode, even if the contact has set the browser preference as Internet Explorer. You can still use Internet Explorer as the browser to access the application.

Manage Contacts Form

The Contact Profile form, accessed by Administrators and Agent/Analysts to create or update the contact record, has been modified to include the locale field. This allows the Administrator or Agent user to set a locale for a new contact record created from the Contact Profile form.

After the contact logs into the application, the application UI will be displayed in the language of the locale selected. Once logged in, the user can change locale preference using the My Profile form.

Searches

Some of the changes introduced to enable effective Searches are listed below.

Keyword Based Search

Keyword based search could throw up unexpected results when executing searches in languages other than English. To enable effective searches through the knowledgebase, and maintain backward compatibility, a new Slice Configuration Parameter '**ENABLE_KEYWORD_BASED_KB_SEARCH**' has been introduced.

If this parameter is set to No, the Keyword tab in the KB Articles screen is hidden and the keyword generation logic would stop. The search mechanism switches to full-text search.

A new action **Regenerate Solution Keywords** has been added in the **Manage Configurations screen** (in the Take Action dropdown list). Executing this action will enable the application to regenerate keywords in all Solutions. This ensures that Keyword based search can be used effectively even if Keyword generation was disabled for some time.

Defined Searches

You can choose to view Defined Search results in other languages. In order to facilitate this, for reflecting localization in existing Defined Searches you will need to prefix the column name with "i18n_". This will need to be manually done by you after the upgrade. For example if the translation of the data of column "status" needs to be enabled then the select list needs to be modified to use "i18n_status" instead of "status"

You will need to prefix each column where translated data is available (or where you want to view the localized data), with "i18n_".

For Personal Searches configured by the logged in user, the select list will continue to be displayed in English, but where localized data is available, the application will implicitly append with "i18n_" for the relevant column.

Note: For the out-of-the-box Defined Searches, selective columns like Ticket Status, Ticket Type etc are prefixed with "i18n_". You will need to manually modify this for any Defined Searches that you have configured, specific to your slice.

Enabling Translations

For enabling customers to create and manage their customized language catalog, the following changes have been undertaken.

Manage Language Catalog

A new form, Manage Language Catalog has been introduced in the Administration Utilities section in the Navigation Menu. This form allows you to define your customized translations.

You can use the Update Elements button on this form to fetch new entries from the predefined areas like Action Names, Templates etc. and update the language catalog. The Key field displays the source text in English. The same is also displayed in the English Text field. The Translation Available field displays information on the languages in which the key has been translated.

You can also manually add a Key to be translated. The Key Field in Language Catalog is case sensitive, that is, the String in application that is to be translated must be entered exactly as used in application. Translations will not be displayed if there is any difference.

Once new translations have been added, you will have to click on the Refresh Cache button to make the translations take effect. If you don't click on the Refresh Cache button the translations will not become available to users as intended.

When providing translations for records like Ticket Template Name and Description, translation for the entire name has to be specified as a single complete phrase.

Bulk Process Data

The Bulk Process functionality has been modified to facilitate import of language translations into the system. A new sheet Language Catalog has been added to the sample sheet that is available for download.

The Sheet Name and Column Names have to be in English. In this sheet, you can enter the key and its relevant translations in different languages.

Font Configuration

Support of fonts in PDF and dashboard charts for Asian languages such as Simplified Chinese or Japanese have limitations around the fonts availability. To overcome this limitation, a configuration file is provided to configure the font path and name installed on the server machine.

The font files are `fontconfig.linux.properties` and `fontconfig.windows.properties` which are placed in the "conf" directory of the application installation. Only one of the fontconfig file needs to be configured depending upon the operating system on which NSD is deployed.

Once the configuration file is updated, you can reload the configurations. For customers undertaking On-Premise installation, the font installation will be a prerequisite before installation. The changes in the properties file for font configurations needs to be changed after the install of the application and before start of the tomcat server.

In absence of accurate configurations or fonts on the system, PDF generation and dashboard charts may get impacted.

Localization of Email Communications

The Application Administrator can setup localized communication templates to enable outgoing communication to be sent as per the locale preference of the logged in user.

To setup this functionality, a Communication Template will need to be configured, with the Locale of the template 'Default'. Then translations can be added in any or all of the supported languages. While the text of the Default template can be in any language, the locale is set as Default.

Note: For System Defined Templates and any Communication Templates available out-of-the-box, a Default template, and translations in supported locales will already be available. You can modify these to fit your communication needs.

The various factors that impact how Incoming and Outgoing Email communication records are handled and viewed in the application are:

- Availability of translated Communication Template for a given locale,

- Locale preference of the logged in user viewing the communication record.
- Locale preference of the intended recipient of the communication record.

This section provides information on various aspects of how communication records are handled in the context of localization.

Generating Outgoing Communication Records

If a communication template is associated with a record, like workflow action, auto-route, SLA threshold violation etc., the following is the expected behavior for how communication records are generated.

- A Communication Record will always be generated using the Default template. If translation for a Communication Template is available in the locale of the intended recipient(s), a communication record will be generated in the language(s) of the recipient(s). If translation is not available, the Default communication record is used.
- When token values are replaced in the Communication Record (replacing actual values in place of the placeholders on the Communication Template), the locale of the Communication Template is considered. Thus, the token values will be in the same language as the communication record.

Note: For Custom Fields, the token values replacement in the locale of the template will be based on whether translation for the Custom Field value(s) is available or not.

If a communication record is manually generated by the Agent/Analyst while working on the ticket (using the Send Mail option or Worklog Send as Mail option), the following is the expected behavior:

- When using Send Mail option, the Agent/Analyst can select the communication template to be used, and select the locale in which the message should be transmitted. The Communication Template lookup will display only Default template. The Agent/Analyst can select the locale in which the communication is to be sent.
- The communication record will be generated in the locale specified by the Agent/Analyst while composing the mail. The locale of the recipient will not be considered.
- If a message is recomposed (based on the action by the Agent/Analyst to regenerate values when the communication is sent at a specified date and time), the current locale of intended recipient(s) is considered when recomposing the communication record.

Transmission of Outgoing Emails

Based on the locale of the logged in user, locale of the intended recipient(s), and the communication records generated, the following is the expected behavior for how communication records are delivered.

- Where corresponding communication records are available in the locale of the intended recipient, the communication record delivered to each recipient will be in their preferred locale.
- When processing Outbound mails, the locale of the recipient will be matched against the locale of the communication record. If the locale matches, the localized communication record will be sent. If not, the default communication record will be sent.
- If the locale of a recipient has been changed after the communication record has been generated and if a communication record is available for the changed locale; the communication is sent as per the new locale of the recipient. If the communication record is not available for the new locale; the Default communication record gets sent.

Processing Incoming Emails

Incoming emails are parsed for keywords in the subject line to decide the action to be taken on the incoming email. Based on the presence of predefined keywords, either an existing ticket gets updated or a new ticket is created.

If the Keywords in the Email subject line are Non-English, then translations must be present in the Language Catalog for the words to be identified as Keywords to related the mail to an existing ticket.

To facilitate parsing of some standard keywords that are used to relate an incoming mail to an existing ticket, or other predefined actions, translations for the following keywords in the supported locales are provided out-of-box. These keywords are:

- SERVICE REQUEST
- INCIDENT
- PROBLEM
- CHANGE REQUEST
- TASK TICKET
- TICKET
- CASE
- RE:

- FW:
- Out of the Office
- Returned Mail
- auto: cn
- mailer-daemon
- undeliverable:
- Approved
- Rejected

The first keyword match determines the locale of the message, and the rest of the message is parsed only for that locale. Based on the keyword match, further action is determined.

Viewing Communication Records

The language in which the communication records can be seen by different logged in users depends on two factors:

- Locale(s) in which the communication record was generated based on availability of translated communication template in one or more supported language and the locale(s) of the intended recipient(s).
- Locale of the logged in user.

Based on these two factors, the following is the expected behavior for how communication records can be viewed.

In the activity tab of the ticket:

- Older communication records (generated before translation for the Communication Template was available) will be seen in the Default language.
- If the logged in user has the locale preference as one of the locales in which the Communication record was originally generated (For example Communication record was generated in Spanish and English and the logged in user has locale preference as Spanish), the user will see the communication in their own language.

- If a logged in user has a locale preference different from the locale in which the communication record was originally generated, (For example, the communication record was generated in English and Japanese and the logged in user has locale preference as Spanish), the user will see the communication in the Default language.
- If a communication record is generated by an Agent/Analyst using the Send Mail or Worklog Send as Mail option, the communication record will be seen only in the Locale to Transmit selected by the agent when sending the communication.
- Trace Logs generated for a communication record will be displayed in the locale in which the communication record was generated.

In Search Communication History:

- The Search Communication History will show records of all communication records that were generated in all languages. Thus, if a communication record was generated in English, Spanish, Portuguese, Japanese and Chinese; the Search for the communication record will show information on each record generated and status of delivery of each record.

For Self-Service User:

- When a Self-Service User views a ticket from the ticket list, if the communication record was generated in the locale of the logged in user, the user sees the record in the same language. If not, the communication will be displayed in the Default locale.
- When the Self-Service User uses the Search Request function, and includes worklog details in the search, all Communication records will be displayed, without considering the logged in user's locale.

For Web Services user:

- The data returned for the Web Services call will be in the locale specified for the web services user. This applies to the activities service on the ticket.

Assumptions and Intended Behavior

This section presents information related to the conditions required for Internationalization and Localization work as expected, and the expected behavior of the application in Internationalized conditions.

Creating and modifying entities

The following conditions apply related to creating and modifying entities and records.

- Administrator is expected to enter primary data in English only and the system will do all language lookups using English as the search key
- Entities in the predefined areas such Work Flows, Templates, Defined Searches etc shall be created and modified by application administrator in English Only. Once the entity is created, the Administrator can add equivalent other language values for fields where the application accepts additional language based values
- Name and Description for Communication Template, Ticket Template, Reports, Defined Searches, Workflow Actions and Task Flow/Group will be looked up against the language catalog and localized on the End User and Analyst Interfaces if translations are made available.
- For Service Feedback, in feedback forms, response Text associated with Radio buttons or Check Boxes are translated only if the translations are included in the Language Catalog.
- Application Setup and Application Utilities entities and records created by the Administrator have to be created in English Only, and in those forms, these records will be displayed in English only.

Locale Selection

Locale Selection is related to the following behavior.

- The Browser locale or the external portal application locale will not have any bearing on the Nimsoft Service Desk locale. The locale from the "User Profile" setting is what will be used by the application for display of the UI and other items.

So user logged in to UMP with Japanese locale can choose to set the locale to Chinese in Nimsoft Services desk, and the application would be rendered in Chinese.
- Internationalization is currently supported only in the Cross Browser mode for the Agent and Administrator User Interface. Currently the application has two modes - IE Specific mode and a Cross Browser mode. Internationalization is supported only with the cross browser version.
- When locale selected is other than English, the Browser preference setting gets automatically set as Cross Browser; even if the logged in user has set the browser preference as Internet Explorer.
- The GUI positioning is as per the minimum default recommended resolution settings that is 1024X768. In lower resolutions, the GUI elements may not be rendered correctly.

Entities Not localized

The following forms or entities are rendered in English Only, and are not being localized.

- Login page will be displayed in English only.
- Session Expiration Message will be in English only as the user locale information will no longer be available.
- Number formats are not localized
- Abbreviations are not translated
- Matching Conditions must be in English. The query has to be in English Only.
- Data Extract- Labels will not be exported in localized language.
- Log output will be in English only.
- Email IDs and domain names will be in English only.
- Licenses will be in English only.
- Enabling Schedulers and Job Triggers will be in English only.

Known Limitations

The list below identifies the known limitations of using Nimsoft Service Desk in localized setting.

- Internationalization works only in cross-browser mode for Agent/Administrator Interface.
- Bold and Italic letters / characters in Asian languages may not be supported
- Knowledge based search would be a full text search. Keyword Based search could show unexpected results.
- Table Sorting functionality is based on character sorting and has been validated only for English inputs. It may not work for other languages.
- Password strength validations, like number of characters, special characters and integers may not work appropriately if the password is specified in a language other than English.
- Passwords may not work for different languages like Chinese/Japanese.

- Spell Checker in different languages is not supported.
- Localized Calendars with Start day of the week or local calendar are not supported.
- Customized Images containing text cannot be localized. Buttons for "Login", "VIP" and "Forgot Password" are in English only.
- Install Anywhere based Installer is not translated. Locale selection is not available during installation.
- Status bar messages are controlled by the browser locale and are not application rendered. However, if the application makes an AJAX request then the status messages would get translated.
- The label caption of the "Browse" button for File Uploads are dependent on the browser and are not controlled by the application
- Confirmation (prompt) dialogs with buttons such as "Ok", "Cancel", "Confirm" are dependent on the browser and are not controlled by the application.
- NSD Gateway integration is not internationalized via web services
- Web service internationalization.
- In Trend Reports covering a Date Range, when data points are based on Months, the names of the months appear in English only.
- Xwiki documentation shall be displayed in English only.

Chapter 6: Layout and Navigation

Overview

To exploit the feature of commonality and to ease the working of the users, a great deal of consistency is maintained across all forms in the application. While individual fields of a ticket would differ based on the requirements of the ticket type, the generic look and feel of the ticket forms are similar.

Similarly, while the layout of individual forms in the Administrative Modules would differ, based on the configuration managed within that section; the layout of the page- with the list of related entities above, and the details area below- is the same across all forms.

The Generic Layout Nimsoft Service Desk Application, with explanation of the layout of the main screens are explained below.

Layout

The generic Nimsoft Service Desk Application layout can be broken into three main components; the Header Section, a left hand Navigation Menu, and the form area where different forms and lists get displayed. You can navigate to any section of the application by going to a relevant link under each section in the Navigation Menu. Details of entries and entities available under a link will be displayed in the Forms Area.

Please note that when you access Nimsoft Service Desk from within Unified Management Portal, you will not see the Nimsoft Service Desk header section and the entities in that section. However, the Navigation Menu and the forms area and all other functionality remain the same.

The Self-Service User Interface layout is different from the Agent and Administrator interface. You can view details regarding the Layout and Navigation of the Self-Service User Interface explained in the Self-Service User Guide.

The application interface for Service Desk Agents is same as that for Administrators. However, Service Desk Agents mostly have access mainly to the Ticket Modules and some added modules like Knowledge Management, Configuration Management etc., as determined by the Application Administrator.

They may also be granted access to Service Feedback module and Trends and Metrics module, depending on the role they perform.

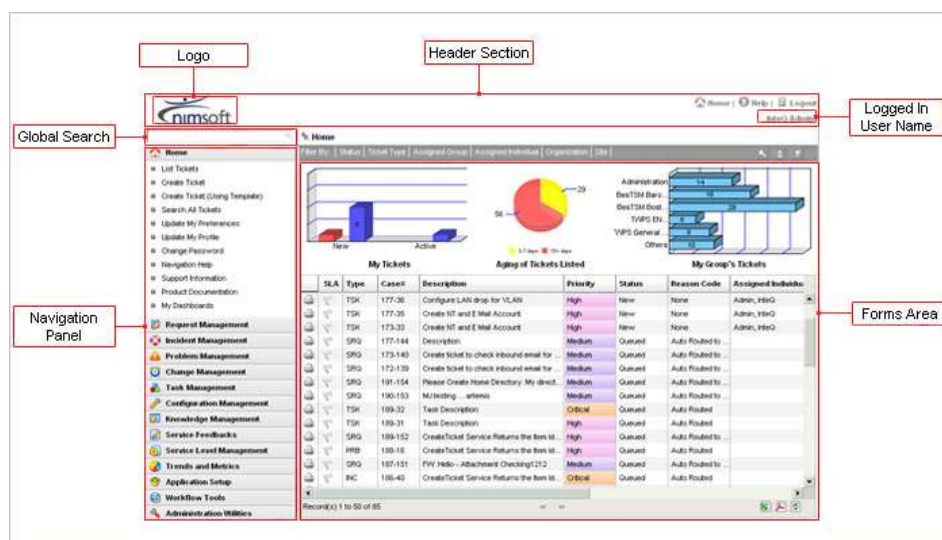
You can view the generic layout of the various forms and lists in the Layout and Navigation Section of the Agent User Guide.

As application administrator, you have access to the entire application, including sections identified as Administrative Modules. The various forms under these sections allow you to configure Nimsoft Service Desk for your Organization specific needs. The generic home layout and layout of the Administrative forms is shown below.

Generic Layout

As application administrator, you have access to the entire application, including sections identified as Administrative Modules. The various forms under these sections allow you to configure Nimsoft Service Desk for your Organization specific needs. The generic home layout and layout of the Administrative forms is shown below.

The generic layout of Nimsoft Service Desk Application has three broad sections - the Header Section, the Navigation Menu and the List Screens. The Header Section and the Navigation Menu are fixed frames for all forms that open in the main window.



Header Section

The header section contains the Nimsoft Service Desk Logo; or as the administrator you can place your organization's logo. The Header section also contains the logged in user's name and icons for accessing the Home Page, Product Documentation, and for logging out of the application.

An important component of the header section is the **Global Search** field. This feature allows agents to search Nimsoft Service Desk for contact records, names, and tickets from across the application. The feature is explained in greater detail under the Search Functionality.

Navigation Menu

The Navigation Menu contains sections and links to the Tickets and Non-ticket modules of Nimsoft Service Desk. You can access common actions like viewing or creating different types of tickets, searching within any ticket module or viewing reports related to that module from the relevant links in the Navigation Menu.

The Application Administrator can control the links under each section in the Navigation Menu. It is therefore possible that the sections you see in the user guide may not be visible in your instance of the application.

Forms Area

The Forms Area displays contents related to the particular links on the Navigation Menu. Hence, depending on the link you are currently at, the screen differs. The four main Screens are Ticket Home screens, Search screens, List Configuration Items screen, and List Solutions screens. These are explained in detail below.

Home Screen

The Ticket Home screen can be accessed from the Home Section and from the List Tickets link under each Ticket Module. The Tickets Home Screen contains the Dashboard that display Ticket Status for the Tickets in the given ticket queue.

The Filter Bar, above the dashboard charts, enables the logged-in user to filter the Ticket List using the various filter options available.

The Ticket List contains details of the Tickets currently in the logged in user's queue

The major sections in the Ticket Home Screen are explained below.

Charts

You can see charts showing tickets by Status , Aging, or SLA Performance and Group(s). As Administrators you have freedom to choose, configure, and view any chart. You can also grant permission to Agent Users to view specific charts that can be of use to them.

The charts are a visual representation of your Tickets queue and you can drill down to group and individual records directly by clicking on the relevant area of the chart. The charts get refreshed to show current data trends.

When you click on any section of the chart, the Tickets matching the section will get displayed in the Ticket List below.

Ticket List

In the Home Page and the List tickets page under each Ticket Module you can see a list of all tickets in your or your group's queue in the Ticket List Area. Each row contains records on one tickets, including the Status, Reason Code , ticket number, description, etc.

You can click on the ticket to view details. The ticket will open in a new window. You can print the ticket via the print icon, or export the list into a PDF or CSV file for reporting and analysis. You can also sort the data according to any column name if you wish to group the list in any particular order.

Filter Bar

The Filter Bar allows you to manage what you see in your ticket queues. By filtering the tickets as per Status, Ticket Type, Assigned to Individual, Assigned to Group, Organization, etc., you can decide which tickets you want to see in your queue as appropriate.

If you wish to view only tickets assigned to you, you can filter the records accordingly to restrict the number of tickets you view. The Filter Bar allows you to set a ticket list that is uncluttered by Tickets that don't need your attention.

You can see details of any highlights applicable for the ticket rows or other symbols like Locked Tickets, etc. from the Legends icon. You can also Reset all filters and restore default filters from the filter bar itself.

The different links in the Home Section allow you to view ticket lists, log tickets, access All Searches to search for Ticket or CI records, view and manage Dashboards, view Product information and Product Help link, view and update your profile and view and manage your preferences.

You can set preferences such as choosing the theme for the application, choosing the Dashboards that are displayed in the Home Screen, row highlighting etc. You can also set default filters for various lists. You can also set your preference for accessing Nimsoft Service Desk on a browser other than Internet Explorer by setting UI Compatibility Mode as Cross Browser.

From the Update my profile link, you can update your personal information, set your preferred Time-Zone and also choose your preferred locale. You can choose to access Nimsoft Service Desk in a language other than English by setting you Locale preference from the available options. This will allow you to view the UI in your preferred language from the available options.

Search Layout

The Search Functionality is available within all Ticket Modules as well as supporting modules of Configuration Management and Knowledge Management. The Search Screen, accessible from the Search Link under each module, has the same layout. The Search Screen contains three tabs- Pre-defined Search, Advanced Search, and Search Results.

The main screens and sections in the Search Screens are listed below.

Search Tab

The Search Tab lists the pre-defined search options made available to users by the Administrator. The Administrator can control the exact item users can search for using the pre-defined search.

This tab will also list any Personal Searches for Ticket or CI records that you configure for your own use.

Advanced Search Tab

The Advanced Search Tab contains various options for you to define your own search. You can search using any single parameter - like Case ID or you can filter the search to display an item matching several parameters.

You can also create and save adhoc search queries as Personal Searches from within the Advanced Search tab. Once saved, the Personal Search becomes available in the Pre-defined Search list along with other out-of-box defined searches.

Search Results Tab

The Search Results Tab displays the search results of either the Predefined Searches, Personal Searched or the Advanced Searches. You can further filter the number or entries to be displayed in the search results list.

List Configuration Items Screen

The List Configuration Items Screen is the Home Screen for the Configuration Management Module. This screen displays the list of Active Configuration Items Records in Nimsoft Service Desk. Filters, to search the CI by CCTI or Status are also displayed.

The two main sections of the List Configuration Items screen are -List Filters and CI List.

The sections on the List Configuration Items screen are explained below.

List Filters

The CI List Filters section allows you to filter the Configuration Items visible to you in the list below. You can filter the list either using the CCTI of the Configuration Item or using the CI Status.

CI List

The CI List contains a listing of all Configuration Items recorded in Nimsoft Service Desk. You can sort the CI list and export the CI List into a PDF or CSV file.

The Solutions List Filters section allows you to filter the Solutions displayed in the list below. You can filter the list based on the Solutions Category, CCTI, Keywords or Symptom Description. After entering the search criteria, you can use the View button to view the solutions list or Clear button to remove the search criteria.

List KB Articles.

The List KB Articles Screen is the Home Screen for the Knowledge Management Module. This screen displays the filters for Knowledge Article. The list below is normally empty. You can enter a search criteria, or enter 'Search' to view all Knowledge Articles.

The list of Knowledge Article matching the search criteria gets listed below. The two main sections of the List KB Articles screen are List Filters and KB Articles List.

The sections on the List Configuration Items screen are explained below.

List Filters

The KB Articles Filters section allows you to choose different filters like KB Article Category, Symptom Description, Keywords, and CCTI. You can enter the filters; or search for all available records.

KB Articles List

The Solutions list gets populated when you enter search criteria or enter view in the Solution List Filter Sections. The Solution List contains a listing of all Solution records available in Nimsoft Service Desk. You can sort the list visible and export the Solutions List details into a PDF or CSV file.

Ticket Layout

All tickets forms (both new tickets and existing tickets) open in a new window. The ticket forms are separate forms and do not have the Header Section and Navigation Menu as the screens of the application.

The screenshot shows the Nimsoft Service Desk Ticket form layout. The form is divided into several sections, each labeled with a red box and a corresponding label on the left:

- Ticket Toolbar:** Located at the top left, containing buttons for 'Create New', 'Copy to Item', 'Save', 'Load Item', 'Print', 'Take an Action', 'Apply Ticket Template', and 'Close'.
- Requester Details:** Located on the left side, containing fields for 'Requester Name', 'Requester Phone', 'Email', 'Organization', 'Site', and 'Location'.
- Affected Service:** Located on the left side, containing a dropdown for 'Affected Service'.
- Request Detail:** Located on the left side, containing a 'Description' field and a 'Details' field.
- Categorization:** Located on the left side, containing a 'Class' dropdown, a 'Category' dropdown, a 'Type' dropdown, and a 'Search CCTI' button.
- Worklog:** Located on the left side, containing a 'Worklog Description' field, a 'Worklog Type' dropdown, a 'Client Viewable' dropdown, and a 'Total Time Spent (HHMM)' field.
- Ticket Details:** Located on the right side, containing fields for 'Request#', 'Status', 'Reason Code', 'Assigned Individual', 'Assigned Group', 'Created On', 'Created By', 'Last Modified', 'Modified By', 'Closed On', and 'Closed By'.
- Prioritization:** Located on the right side, containing dropdowns for 'Source', 'Impact', 'Urgency', and 'Priority'.

While each tickets would have specific fields, depending on the needs of the specific ticket type, broadly the tickets contain:

- Ticket Toolbar - which allows the logged-in user to take actions on the ticket
- Requester Details - which contains details of who has raised the request (and for whom)
- Ticket Details - which contains the Ticket ID, Ticket Status and other auto-populated details
- Request Details - which contains details of what service or action is being requested
- Prioritization Fields- which allow the logged-in user to set priority for the ticket
- Categorization Fields - which allow the logged-in user to categorize the ticket

- Worklog Section - which allows the logged-in user to update work done on the ticket

Admin Module Form Layout

Forms in Nimsoft Service Desk allow the Administrator to set up the service desk and configure the various modules within. The layout of the forms have a great deal of consistency though there are some differences to allow specific actions for different forms.

You can access Forms from any link under the Workflow tools or Application Setup. For example, to manage or configure Contacts, select Manage Contact from the Application Setup option to see the Manage Contacts Form.

The screenshot shows the 'Application Setup (Manage Contacts)' form in Nimsoft. It features a left-hand navigation panel, a top header section, a main table of existing contacts, and a detailed form for editing a selected contact.

ID	Full Name	Phone Details	Phone Numbers	Email	Job Title
1	Admin, Integ	Business	1-781-590-6656	admin@integnet.com	Admin, 1000
53	Breuer, John	Company	1-646-789-8348	JBreuer@vps.com	CEO
54	Lombardo, James VPE@	Business	1-646-789-8324	VPE@vps.com	VP Engineering
55	Lien, Timothy	Business	1-312-687-4542	VPE@vps.com	VP Marketing US-EU
56	Lookin, Anthony	Business	1-734-789-7787	VPE@vps.com	VP Mktg
57	Kent, Vincent	Company	44-020-326-9887	SSU@vps.com	CM UK
58	Schulte, Donald ITM	Business	49-765-967-8997	ITM@vps.com	IT Change Manager
59	Huber, Allen	Business	85-222-346-7885	VPE@vps.com	VP-SEA
60	Stegler, Neil	Business	852-234-686-9826	SSU@vps.com	RM HK

Below the table is the 'Item Details Form' for a selected contact (John Breuer). It includes fields for Title, First Name, Last Name, Email, and various contact details like phone numbers, address, and employee information.

The two sections in all Administrative Forms are Existing Items List and Item Details Form.

Existing Items List

The Existing Items List on all administrative forms consists of a list of all entities and items related to each administrative form. For example, if the form being accessed is Manage Contacts, this Existing Items list will contain a list of all Existing Contacts.

A Filter Bar will allow you to filter the items listed in the table below. The filter options available in each administrative form differ depending on the entities managed in that form.

To view the details of an entity in the list, you can click on the item; all details related to that entity will get populated into the form below.

Item Details Form

The section under the table displays a blank form to configure new entities related to that section, with the Create New Button activated. Initially, only one tab is activated in the configuration form, but once the record is created and saved, other tabs specific to a form get displayed, and allow the user to fill in details as required.

You can also modify an existing item. Clicking on the item in the List above will populate details related to that item. The various aspects that can be modified can be seen in the form; and modified appropriately from the various tabs on the record form.

Navigation

You can navigate through Nimsoft Service Desk via the Navigation Menu to view appropriate link under each section. For example, if you wish to configure a Contact Record, you can find Manage Contacts link under Application Setup in the Navigation Menu. Clicking on this link will give you access to the Manage Contacts form.

Filter Lists

All lists in the administrative modules can be filtered using the available Filter Options. Common filter options for most forms are:

- Filter by Status (Active/ Inactive) where a record can be made inactive;
- Filter by Type (System-Defined and Non-System Defined)

Other filter types relevant to the specific record type will be displayed in the respective form. You can use these to narrow your search and navigate to the appropriate record.

Chapter 7: Administrative Modules

Overview

As the application administrator, you will be involved in setting up Nimsoft Service Desk for your Organization; and enabling the key features of the application for Self-Service Users and Service Desk Agents.

The Administrative Modules - Application Setup, Workflow Tools and Admin Utilities - enable the Application Administrator to configure the application as per the requirements of the organization.

This section identifies the links within each administrative module and explains the actions you can take related to each. Further details on how the links are used to enable a particular feature or functionality are explained in the other relevant sections.

The table below identifies the sections that allow you to configure the application and manage the application functionality. This includes sections and links to forms that allow you to configure various records in the system and set up the application as per the needs of your organization.

Further information about the actual forms listed here; and how the application can be configured are explained in the other sections of this guide.

Setup of Configuration Management, Knowledge Management, Service Feedback and Service Level Management is explained in the respective sections.

Application Setup

The links under Application Setup section enable you to perform most tasks necessary for Preliminary Setup of the application. This includes taking actions related to building the initial records into the application and undertaking the ground work for enabling ticketing functionality. Each link in the Application Setup Section, and the various actions you can take from that section are listed below.

Manage Organization

This link enables you to view Organization records and create new organization records. Nimsoft Service Desk enables you to build a three level hierarchical Organization record for each organization in your instance; with Organization at the top level, multiple Sites under an Organization and multiple Location under each Site. You can create multiple organization records (for support users, support providers, channel partners, vendors, etc.) within your instance of the application.

Some of the actions you can take related to Managing Organization are:

- View existing organization records, using filters to expand or contract the list.
- Create new Organization records as per the needs of your IT Support activities.
- Configure geographical or functional Site for each Organization .
- Configure geographical or functional Location under each site.
- Relate contacts to the organization.
- Associate a time-zone for each site; as default Time Zone for contacts associated with the Site .
- Control (enable or disable) ability of all contacts related to the organization to participate in Service Feedback process.
- Manage Organization (or site or location) status Active /Inactive.
- Terminate an Organization by removing all transaction data and also delete all other dependent data related to the terminated organization.
- View dependent data from the Dependent Data tab with a list on the dependent entities, their description, the action on termination, and the "Number of records" for each. You can drill down to view the list of each dependent entity.

Manage Contacts

This link enables you to view existing Contact Records , create new contact records, and manage contact records. Creating contact records for all those associated with the IT Support services as service users, service providers, vendors, etc., enables effective relationship of the support requests to the contact who request the service.

Some of the actions you can take related to Managing Contacts are:

- View existing Contact Records ; using available filters to expand or contract the list.
- Create New contacts, Update existing contacts or Delete existing contacts.
- Associate a contact to organization, Site , and Location .
- Determine time-zone applicable for the contact.
- Manage system login to decide whether a contact is to be given system access or not.

- Decide which License Type is to be assigned to a contact - Fixed , Floater , or Self-Service User.
- Enable or disable access to 'View Organization Tickets' for contacts marked as Self-Service User .
- Mark Contact as VIP Users ; associate PIN Authentication for contacts.
- View groups or roles the contact is associated to; and add the contact to groups orRoles .
- View Configuration Items related to the contact.
- View Open tickets related to the contact.
- View, create, update, or delete special notes or attachments to a Contact Records .
- Manage contact status (Active or inactive).
- View dependent data from the Dependent Data tab with list of records on dependent entities, their description, the action on termination, and the "Number of records" for each. You can drill down to view the list of each dependent entity.

Manage Support Groups

This link enables you to manage Support Groups for different type of activities related to IT Support. Grouping contacts into support groups allows you to manage Permissions more effectively.

A support group, consisting of all members who undertake similar type of activities enables managing service desk tasks and service delivery more effectively. A contact can be associated with multiple groups, with any one group being set as Primary Group.

Some of the actions you can take related to Support Groups are:

- View existing Support Group details using filters to expand or contract the list.
- Create new Support Group, update existing Support Group, Delete existing support group.
- Relate contacts to Support Groups or remove contacts related to a support group.
- Set the Support Group as Primary Support Group for a contact related to the group.

- Define whether the Support Group can be used for Permissions , Notification , Assignment, Approval, or SLA Escalation based on activities done by the groups.
- Determine Business Hours for Support Groups by associating Schedules to the support group.
- Create, update, or delete Support Group Business Hours schedule for different days of the week.
- Associate a Holiday List to a Support Groups .
- Control ability of a group and associated contacts to participate in the Service Feedback process.
- For Self-Service Group; enable or disable ability to View My Organization Tickets.
- Manage Status of Support Group (Active/Inactive).

Manage Roles

This link enables you to Manage Roles. A Role could be created using members of multiple Support Groups and/or individual contacts. Creating roles simplifies management of permissions at the Role level.

Some of the actions you can take related to Roles are:

- View existing role - using filters to expand or contract the list.
- Create New role, update existing role. or delete existing role.
- Relate Contacts and/or Support Groups to a role.
- View Permissions assigned to the role.
- Manage status of a role (Active/Inactive).

Manage Holidays

This link allows you to manage details of Holidays in the yearly calendar. A Holiday Group can be related to several entities in Nimsoft Service Desk, like Support Groups, Auto-Route , etc.

Some of the actions you can take related to Mange Holidays are:

- View existing Holiday groups.
- Create new holiday groups, Delete existing holiday group.
- Add new holidays to existing Holiday Group, delete existing holiday from a holiday group.
- Define whether a holiday is to be renewed yearly.
- Manage Holiday Groups (Active/Inactive).

Manage Categorization

This link enables you to manage Categorization applicable for different ticket modules and configuration management. Nimsoft Service Desk enables a hierarchical four level categorization of tickets and Configuration Items .

You can create Class, Category, Type, and Item level categorization applicable to different forms. While you don't have to create a categorization record at all four levels, you have to define at least a Class for each record.

Some of the actions you can take related to manage categorization are:

- View existing categorization records using available filters to expand or contract the list.
- Create new Categorization record, update or delete existing categorization record from the list.
- Relate categorization record to multiple ticket or configuration item forms.
- Associate new or existing image with CCTI.
- Manage status of an existing Categorization record (Active /inactive).

Manage Attributes

This link enables you to create pool of Attributes with unique attribute names. Attributes from this pool can be used when creating custom field on tickets and as attributes in CI Attribute templates.

Some of the actions you can take related to managing attributes are:

- View existing attributes; using available filters to expand or contract the list.
- Create new attributes, Update existing Attributes details.

- Define Attribute type, sort order and possible values for the attributes. These values get carried over to the templates where attribute is used.
- Define Attribute type of text or multi-line text that support upto four thousand characters.
- Create an attribute type as Section Header to enable grouping of custom fields in tickets.
- Delete existing Attributes (Note that you will not be able to delete attributes that are already in use on other existing records).

Manage CI Attribute Templates

This link enables you to manage CI Attribute templates. A CI Attribute Template allows you to add Attributes over and above the generic available attributes and fields, to a CI Record. This is needed where an attribute value specific to a CCTI is not available as a field on the system defined CI record form.

Some of the actions you can take related to managing CI Attribute Template are:

- View existing CI Attribute Templates.
- Create new or update existing CI Attribute Templates.
- Add new Attributes to default system defined CI Attribute Template.
- Add new Attributes to existing non-system defined CI Attribute Template .
- Determine whether the attribute is to be applied to existing CI records.
- Determine whether the attribute value is to be applied during CI Record creation.
- Determine whether use of unique value is to be imposed for an attribute.
- Relate CCTI (Categorization) of CI to which the CI Attribute template gets applied.
- Manage CI Attribute Templates status (Active/Inactive).

Manage Custom Fields

This link enables you to manage custom fields for tickets. Custom Fields enable you to add standard fields to the ticket forms. These fields allow you to solicit additional information that would assist in effective processing of tickets.

Custom fields on tickets can be viewed on both Self-Service User Interface (if accordingly set) and in Agent Interface; custom fields can be used for setting Auto-Route and workflow actions.

You have to use appropriate Attributes from the Manage Attributes Pool to create custom fields on tickets.

Some of the actions you can take related to managing Custom Fields are:

- View available custom field template; using available filters to expand or contract the list.
- Create new custom field template or update existing custom field templates.
- Add attributes to a custom field template or remove attributes related to a custom field template.
- Group Custom Fields attributes into sections using section headers.
- Enable or disable Self-Service Users ability to view custom fields on the ticket template.
- Mark a custom field as Required Field, ensuring value is updated when ticket is saved.
- Relate Categorization record (CCTI) to the custom field template.
- Manage Custom Field Templates update, modify, or delete a custom field template.

Manage Config Parameters

This link enables you to view Slice Config Parameters and modify parameter values as per your needs. The Configuration Parameters enable you to turn on or turn off a functionality; or manage how a functionality is applied in your Organization.

Some of the actions you can take related to Configuration Parameters are:

- View available Configuration Parameters using available filters to expand or contract the list.
- Select a parameter that you wish to modify.
- Update or modify parameter values to choose alternate, acceptable values.

Bulk Process Data

This link enables you to Bulk Process data into the application. You can undertake a bulk process of Organization , Site , Location , Contact, Support Groups , Role , Categorization , and Configuration Items records after gathering all required information in the appropriate format. The Data to be bulk processed has to be stored in an MS Excel file.

Some of the actions that you can take related to Bulk Process Data are:

- Specify the file Location on your local system from where the data is to be uploaded; and map the records to the appropriate sheet, and subsequently, appropriate columns in the database.
- Import data into the application database as newly created data.
- Update existing data.
- Delete existing data.
- View progress of the bulk process.
- View details of records that were rejected.
- View import logs to identify errors leading to records being rejected; so as to make corrections and undertake upload of missing records.

Manage Charts

This link enables you to Manage Charts that can be viewed on the user interface. You can use the charts as part of dashboards visible on the Agent and Administrator interface.

Some of the actions you can take related to Manage Charts are:

- View available charts using filters to manage the list visible.
- Create new charts, defining the various parameters related to the chart.
- Update or modify existing charts.
- Manage permissions for support groups, roles, or contacts to access charts.
- Manage charts status (active or inactive).

Manage Dashboards

This link enables you to Manage Dashboard that can be viewed by Service Desk Agents of Administrators in their user interface.

Some of the actions you can take related to Dashboard are:

- View existing dashboards using filters to manage the list.
- Create new dashboards, defining the various parameters related to the dashboard.
- Update or modify existing (non-system defined) dashboards.
- Manage permissions for access to the dashboard for contacts, support groups, or roles.
- Manage dashboard status (active or inactive).

Manage Configuration

This link enables you undertake slice configuration activities like enabling Email functionality, setting up Job Triggers etc.

Some of the actions you can take from the Manage Configuration link are:

- Take actions like Purge Transaction, Delete Inactive records, Reload Slice Definition, or Remap Imported CI Attributes when required.
- Select time a session can remain idle before the server terminates the session automatically.
- Choose the complexity level of password.
- Renew or add licenses using the license key received from Support.
- Set up inbound and outbound email configurations.
- Create and schedule Job Triggers for background jobs taken up periodically by the application.

Workflow Tools

The links under Workflow tools enable you to set up the ticket modules and ticketing functionality as per the support processes specific to your Organization . You can perform actions related to managing workflow actions, auto-routes, configure Approval groups, templates, and take up advanced configuration activities like managing defined searches and Schedules .

Manage Communication Templates

This link provides access to the Manage Communication Templates form. You can create communication templates for various automatic and manual Notifications from the application. You can perform various actions related to managing Communication Template from this link.

Some of the actions you can take related to Communication Templates are:

- View existing Communication Templates using filters to manage the list
- Create new communication templates by relating the template to multiple ticket and non-ticket forms, specifying the fields on the communication template
- Modify existing Communication Templates ; change place holders, forms and update the template
- Manage (grant or revoke) Permissions to access communication template for contacts, support groups and roles

Manage Workflow Actions

This link allows you to manage workflows for the different actions on tickets. The Workflow Actions configured here get applied to tickets and enable the tickets to be progressed towards resolution and closure.

Some of the actions you can take manage Workflow Actions are:

- View existing workflow actions using available filters to manage the list
- Configure new workflow actions, relating the action to a ticket type
- Determine whether any special function has to be associated with the workflow action
- Create / modify/ delete Matching Conditions (fields and values) configured for a Workflow action
- Define Set Field values, which get set when a workflow action is executed

- Specify Fields to be validated as Required when Action Options is executed
- Relate and unrelate one or more communication templates for notification or a workflow action execution
- Manage permissions to the Workflow Actions for contacts, support groups and roles
- Manage workflow action status (active/inactive)

Manage Auto Routes

This link allows you to manage Auto-Route for assignment of tickets and initiation of some workflow actions on tickets.

Auto-routes get applied the first time a ticket is saved. Configuring auto-routes enables routing tickets based on specified Matching Conditions , to specific Support Groups . This enables overriding the default routing defined in the slice configurations.

Some of the actions you can take to manage Auto Routes are:

- View existing auto-routes using available filters to manage list
- Configure new auto-routes by specifying the ticket type it gets applied to, defining the auto-workflow action that gets applied, setting a sort order for the Auto-Route , etc.
- Update or modify and existing auto-route; by changing any field values
- Define Matching Conditions that get applied to an auto-route
- Define field values like status, reason code, phase, etc. to be set when the auto-route gets applied
- Associate communication templates for notifications to stakeholders when an auto-route is applied
- Associate a schedule- calendar horizon, days applicable, and time-zone, to an auto-route
- Associate Holiday list to an auto-route - specify auto-route to be applied only on the Holiday list; or holiday list to exclude the Auto-Route
- Manage Auto-routes status (Active or inactive)

Manage Approval Groups

This link allows you to manage approval groups that are used as part of the Approval Process.

Configuring approval groups for different types of changes facilitates effective submission of a ticket for Approval or review and configuring an effective Approval mechanism.

Some of the actions you can take manage Approval Groups are:

- View existing Approval Groups using filters to manage the list
- Create new Approval Group; specifying required values; or modify existing approval group
- Define matching conditions to be applied when selecting an approval group for a specific change
- Associate Approvers and Reviewers with the approval group
- Associate Contextual Approvers/Reviewers (like Requester , manager, etc.), if appropriate
- Enable or disable agent's ability to modify approvers' list on use
- Manage Approval Groups Status (active or inactive)

Manage Ticket Templates

This link allows you to manage Ticket templates. You can configure Ticket Templates, with pre-populated fields for standard, oft repeated requests; and make these available for Self-Service Users and/or Service Desk Agents . This reduces User effort in logging the request, and more effective auto-routing of the ticket.

Some of the actions you can take to Manage Ticket Template are:

- View available ticket templates; using filters to manage list.
- Create new ticket templates specifying template name and associated with ticket type
- Modify or update existing Ticket Template to make changes to the fields or values associated to the template
- Define Auto-Routes for the ticket template, and specify whether this should override other auto-routes

- Identify Set Field Values that need to be automatically available when the ticket template is accessed
- Manage (grant or revoke) permissions for access to the ticket template to contacts, support groups and Roles

Manage Task Groups

This link allows you to manage new Task Group for Task tickets. Configuring a task group for tasks that are to be undertaken as part of a specific request fulfillment activity; for example New Recruit Provisioning related tasks; enables management of all Tasks as part of a specific task group.

Some of the actions you can take to Manage Task Group are:

- View existing Task Groups using filters to manage the list
- Create new Task Group , associated to a ticket type, name and description
- Modify existing task group, adding or removing tasks from the group and managing the Task Order
- Modify tasks associated to a Task Group, associate auto-assign action and enable ability to auto-assign on create
- Manage permissions for access to a task group to contacts, support groups and roles
- Manage Task Group status (active or inactive)

Manage Task Flows

This link allows you to manage Task Flow . When a series of interdependent activities, need to be undertaken towards resolution of an open ticket, a Task Flow can be configured. This enables effective management of all tasks that need to be down towards request fulfillment.

A Task Flow can be created with a combination of one or more task groups and/or individual tasks.

Some of the actions you can take to Manage Task Flows are:

- View existing Task Flow using filters to manage the list
- Create a new Task Flow, associated to a ticket type, name, and description
- Modify existing Task Flow, add and remove individual tasks or task groups from the task flow, associate Task Order to determine Task Flow sequence

- Define action on success and action on failure to associate a workflow action to success or failure of a task in the task flow
- Manage (grant or revoke) permissions for access to a Task Flow to contacts, support groups, and roles
- Manage Task Flow status (active or inactive)

Manage Defined Searches

This link allows you to Manage Defined Searches . Configuring a defined search eliminates the need for create a new search query every time a search is to be executed.

You can manage access to system-defined searches or create new Defined Searches as per the search requirements in this section.

Some of the actions you can take related to Defined Searches are:

- View available defined searches, using available filters to manage the list
- Create new Defined Search by specifying required details and constructing the search query
- Update or modify existing defined search query and preview the result to check output
- Manage (grant or revoke) Permissions for access to the defined search for contacts, support groups, or roles
- Manage Defined Search status (Active or inactive)

Manage Schedules

This link allows you to manage schedules for routine service desk activities. In routine operations related to managing the IT Support services, Service Desk Agents could be required to perform some routine activities like taking data backups, generating reports, etc.

For such repetitive tasks performed against a pre-determined schedule, you can create schedules. Nimsoft Service Desk will auto-create tickets against the Schedule and assign the ticket per the Schedule to an identified resource or Support Groups .

Some of the actions you can take related to Manage Schedules are:

- View list of Active schedules or search for a schedule from the list
- Create a new schedule by specifying the schedule owner and schedule details like start and end date and execution time

- Associate a weekly calendar, holiday list, Time Zone , and re-occurrence pattern with a Schedules
- Determine routing of a schedule ticket; override auto-assignment, if required
- View Schedule logs to review status and progress
- Manage Schedule Status (active or inactive)

Manage Value List

This link allows you to access the editable value list. Nimsoft Service Desk allows you to modify Values of ticket fields like Priority , urgency, source, etc., to be more in sync with your own value conventions for these fields. You can modify the Value list to choose different acceptable values.

Some actions you can take related to the value list are:

- View Value list items that can be managed or modified using filters to manage the list
- Modify value options form the available options, as appropriate
- Modify value option sort order to manage visual layout of the field

Administration Utilities

The links available to you under Administration Utilities section assist in the routine activities of managing the application for other Users and assisting the Self-Service Users and Service Desk Agents in their use of the application.

Some links in this section also enable you to manage permissions for specific actions and functions.

Reset User Password

All Users , including Self-Service Users and Service Desk Agents can manage their own password, such as changing their password form the user interface. The Reset User Password link enables you to provide a system generated or manually created password for users.

The actions you can take from this link are:

- Manually reset user password by tying in new password in the given field
- Reset password to provide a system generated password for the user. Users get email Notification about the password being changed/reset.

Manage Sessions

When a User logs into the application, a session is activated. You may need to forcibly terminate an Active session. You can do so using Manage Session link.

The actions you can take from this link are:

- View list of all active Session and details of all logged in users
- Terminate an active session by logging out the user

Manage Ticket Locks

A ticket that is open and being modified by a logged in user, or a ticket submitted for Approval (if so configured) gets locked. A locked ticket becomes Read Only; and cannot be modified by another user.

You may need to unlock locked tickets to allow progression of the ticket. You can unlock tickets from the Manage Ticket Locks link

The actions you can take from this link are:

- View a list of all locked tickets and details of who locked the ticket and when
- Unlock a locked ticket by removing the ticket lock

Manage Toolbars

You can manage the options available on Toolbar of tickets, Configuration Items and knowledge articles. This manages the ability of Users to view and access that option on the toolbar. This can be done from the Manage Toolbar link.

The actions you can take from this link are:

- View a list of toolbar items using available filter to manage the list visible
- Manage (grant or revoke) permission for a toolbar option for contacts, support groups, and roles
- Create new toolbar items using appropriate code
- Modify sort order of toolbar item, as required

Manage Navigation Menu

You can manage the sections and links within each section available in the Navigation Menu for Self-Service Users and Service Desk Agents. This manages the ability of Users to view and access that link or action in the Navigation Menu. This can be done from the Manage Navigation Menu link.

The actions you can take from this link are:

- View a list of Navigation Menu items using available filter to manage the list visible
- Manage (grant or revoke) permission for a Navigation Menu option for contacts, support groups, or roles
- Create new Navigation Menu items using appropriate code
- Modify sort order of Navigation Menu item, as required

Manage Report Configurations

Nimsoft Service Desk provides access to a wide range of pre-configured out-of-the-box reports. You can manage the ability of different users to view and access these reports from Manage Report Configurations link.

The actions you can take from this link are:

- View a listing of available reports, using filters to manage the list
- Modify report configurations, changing report description, related to form, etc.
- Manage (grant or revoke) permissions for access to pre-configured reports to individual contacts, support groups, and Roles.

Search Communication History

Nimsoft Service Desk stores a record of all incoming and outgoing communication to and from the application. During routine operations, you could be required to view the communication history, or delete a scheduled communication. You can do so from the Search Communication History link.

The actions you can take on this link are:

- Define search parameters and search for a communication record
- View details of a search records matching the search criteria
- Extract details of communication search list into PDF or CSV file

- View details of a chosen record to see detailed communication
- Delete a communication if it is scheduled

Manage Logon Notice

As Application Administrator, you can set up a maintenance notice if Nimsoft Service Desk is being taken down for a planned/scheduled maintenance.

The actions you can take from this link are:

- Create a message to be displayed on the Home Screen indicating a planned outage of the application.
- Enable a notice to be displayed for a specific duration when the application will be unavailable.
- Disable the notice when the maintenance notice is no longer applicable.

Predefined Searches

Nimsoft Service Desk provides out-of-the box defined searches for administrative records related to Organization, Site and Location.

The actions you can take from this link are:

- Execute a defined search from the available pre-defined searches
- View the results of the search in the results tab
- Export the list generated by the search into PDF or CSV files.

Access to all Administrative Modules and to the whole suite of the Application functionality is available by default to all contacts who are members of the System-Defined Administration Support Group. By default permissions to all entities and records that are configured are available to the Administration Support Group.

When the Nimsoft Service Desk Instance is configured; one contact is configured as Administrator for the Slice. Other contacts can subsequently be added to the this group by relating contacts to the Administration Group and making it the Primary Group of those contacts.

Manage Language Catalog

The Manage Language Catalog section allows you to create and update the customized language catalog for custom defined entities in your own slice.

The actions you can take from this link are:

- Refresh the form to collate all custom defined values like Attributes, Communication template messages etc.
- Select a custom value to be translated and provide translation for the selected text string
- View strings of translated text (if translation has been done) for a selected text string.

Access to all Administrative Modules and to the whole suite of the Application functionality is available by default to all contacts who are members of the System-Defined Administration Support Group. By default permissions to all entities and records that are configured are available to the Administration Support Group.

When the Nimsoft Service Desk Instance is configured; one contact is configured as Administrator for the Slice. Other contacts can subsequently be added to the this group by relating contacts to the Administration Group and making it the Primary Group of those contacts.

Chapter 8: Manage Configuration

Overview

After Nimsoft Service Desk has been installed On-Premise; or the application slice has been created for users in the SaaS mode, the Application Administrator has to undertake some actions for the initial setup of the application instance.

This includes setup of the Email functionality, creating and enabling background Job Triggers etc. to configure actions that get across a given application instance.

The Manage Configuration Form, accessible from the Application Setup module, allows you to undertake configurations needed to set up your instance of Nimsoft Service Desk and some additional actions related to your instance. These actions are explained below.

Manage Configuration Actions

To access the Manage Configuration form, login to the application and navigate to the Application Setup section in the Navigation Menu. Click on Manage Configuration link to open the slice configuration management form.

Application Setup (Manage Configurations)

Slice #1000

Slice Information

Slice# 1000 Slice Description IntraDesk Slice# 1000 --Select-- Take Action

Notes dddd

Slice Details

General Information Licenses Single Sign On Inbound Email Outbound Email External Notification Job Triggers

Database Server Name Database Server Port Database Schema Name

mayabusa.engg.baroda.inteq.smartweb.com 1433 QA_ServiceDesk_Quickstart_v6_1_0_3

Report Database Server Name Report Database Server Port Report Database Schema Name

mayabusa.engg.baroda.inteq.smartweb.com 1433 QA_ServiceDesk_Quickstart_v6_1_0_3

Homepage URL

Self-Service Homepage URL

web/self-service/ssp/home.jsp

Session Timeout Slice Token Password Strength

60 slice1000 Level 1

Licenses Details

Fixed Licenses Count	Floater Licenses Count	Self-Service Licenses Count	Web Services Licenses Count
200	200	200	1

The Manage Configuration Form displays the Slice Number as a Read Only field. For customer using Nimsoft Service Desk as SaaS customers, the Slice number is unique per customer, to secure the data in your slice.

For customers using Nimsoft Service Desk On-Premise installation, Slice Number is not unique, as this is not needed for securing the data in the same way as it is used in SaaS mode. The Slice Number field is not editable and appears as a Read Only field.

The Slice Description field can be used to provide any information useful for your slice. However, this field is not mandatory. Similarly, you can add any relevant notes in the Notes field; which is also not a required field.

The Take an Action field is a dropdown field that allows you to take some actions at the slice level. These actions are explained in the table below

Action	Explanation
Purge Transaction	This action allows you to remove all Tickets from your instance of Nimsoft Service Desk. The action is not reversible. If you select this action, the application will display a message informing you that the transaction data cannot be recovered. If you confirm the action, all Ticket transactions including ticket history, SLA records, worklogs, ticket relationship with other tickets, Configuration Items, Solutions, Attachments etc., will get removed.
Delete Inactive Records	Many forms in Nimsoft Service Desk like Workflow Actions, Auto-Routes etc. allow you to make records inactive if you do not wish to use a record that is created. You can use the Delete Inactive Records action to permanently delete inactive records. However, Deprovisioned CI records are not removed when this action is executed.
Reload Configurations	This action reloads the slice configuration. When you select this option and execute it, all changes made to the slice from the back-end, like enabling Job Triggers, Email Configurations etc. get enabled and get applied to your instance of the application. The changes get reflected on the application interface.
Reload Slice Definition	This action will reload the slice specific configurations like Session Time Out, Password Strength etc. that have been changed in the General Information tab. You can also execute this action to ensure any data changes made at the back end get reflected in the slice.
Remap Imported CI Attributes	This action maps all new CI attributes that have been imported into the slice via bulk upload process, to existing CI attribute templates. This ensures that all CI Attribute Templates are updated appropriately.
Regenerate Solution Keywords	This action can be used to regenerate Keywords on Knowledge Articles created when the Keyword Generation functionality was disabled for any reason. This ensures that Keyword based search can be used effectively even if Keyword based search was disabled temporarily for

	some reason

The tabs in the Manage Configurations form, and the function managed by within each tab are explained in the sections below.

General Information Tab

The General Information tab allows you to edit or configure some aspects of the slice like manage password strength, manage session time-out and other such aspects related to how your instance of Nimsoft Service Desk will function for all users.

Some of the information in this tab are read only fields; and provide you with information that can be used for reference when interacting with Service Desk Support if you face any issues.

When the Manage Configuration form opens, the General Information tab is displayed by default.

The editable fields in the General Information tab; and a brief explanation of these fields are given in the table below.

Field	Explanation
Session Timeout	Session Timeout allows you to define the number of minutes that a session can remain idle before the server automatically terminates the session. The default time is 60 minutes. You can either increase or decrease the time as per your organizational conventions.
Slice Token	This is the unique authorization token that is used by external systems like Contact Sync module, Single-Sign-On etc. to communication with Nimsoft Service Desk. A default Slice Token is assigned when the slice is created. If the value is changed, the change must be noted and entered in external applications where Slice Token is used.
Password Strength	You can define the complexity level of password. You can choose from the following: Level 1: Password must be at least 8 characters long Level 2: Level 1 + Password must be a combination of upper and lower characters Level 3: Level 2 + Password must contain at least one numeral Level 4: Level 3 + Password must contain at least one special character

Other fields in the General Tab are read only fields. Fields like Database Server Name, Database Port, Database Schema Name, Report Database Server Name, Report Database Port and Report Database Schema name are Read Only fields.

You may need information in these fields when contacting support for assistance.

Licenses Tab

The Licenses tab displays a list of licenses authorized for slice. There are 4 types of licenses: Fixed , Floater, Self-Service, and Web Services. In addition, a platform license – service desk is also provided.

You can access Licenses from the Manage Configuration link under Application Setup. Clicking on the tab opens the Licenses Form.

The screenshot shows the 'Licenses' tab selected in the 'Manage Configuration' window. The table displays the following data:

Module	Authorized for Com	Authorized IP Address	# Users	Valid Until	License Code
servicedesk	Nimsoft	*	1	16-may-2012	CHOW WHO THE CEL TACK GIBE
servicedesk_fixed	Nimsoft	*	200	16-may-2012	MULE BIND CLOG EVE BUY DOW
servicedesk_floater	Nimsoft	*	200	16-may-2012	RUDE WORK CHOU PAR RUN EGAN
servicedesk_selfservic	Nimsoft	*	200	16-may-2012	AM TOGO GAL NOOK KONG VEAL
servicedesk_webserv	Nimsoft	*	1	16-may-2012	CUE BELL BURR GELD RUNG LUKE

Record(s) 1 to 5 of 5

Below the table is a text area labeled 'License Key(s)' and an 'Add License' button.

The table in the Licenses tab displays information about the types of licenses available, the number of each license type, the company the license is authorized to, the IP address of the machine(s) on which the application is deployed, license validity and license code.

When the service desk slice is created, a default license of 30 days is associated with the Slice. Within these 30 days you will have to renew the licenses or else the system gets locked and is inaccessible.

Starting seven days before the Expiry Date for the License, the Application displays the following notice every time when an Application Administrator logs into the Service Desk Application:

“To continue using the Application without interruption, Licenses must be renewed at the earliest by contacting Nimsoft. Nimsoft Support shall send a License Key via Email. You can use this to renew or add the licenses.”

Nimsoft Service Desk Support sends out an email with the license keys. You can copy paste the relevant information in the License Key field in the Licenses Tab and click on Add License. The licenses get related to your slices, and the relevant information gets refreshed in the tables above.

Single Sign On

Nimsoft Service Desk provides the ability to authenticate users with an Identity Provider by using a Single Sign-on application. The SAML 2.0 based Single Sign On feature allows users to login seamlessly into NSD without being prompted for network or NSD username/password.

You can choose whether you want to enable SAML 2.0 based Single Sign On or not. If you wish to configure the SAML 2.0 SSO, you will need undertake setup and configuration on your Identity Provider Server as well as in the Single Sign On Tab shown below.

The screenshot shows the 'Single Sign On' configuration tab. It includes a checkbox for 'Enable SAML Single Sign On?' which is checked. Below it are text input fields for 'Authorization Domain' (containing 'twps.com'), 'Identity Provider Login URL' (containing 'https://godzilla.engg.baroda.inteq.smartweb.com/adfs/'), and 'Identity Provider Logout URL'. A large text area for 'Identity Provider Certificate' contains a long alphanumeric string. A red box highlights the 'Single Sign On Form' label below the fields.

The table below identifies the fields available on the Single Sign On form

Field	Explanation
Enable SAML Single-Sign On (checkbox)	A Check Box that enables the Single Sign On feature.
Authorization Domain	This is a required field and it defines the the domain to be used for NSD-SSO application instance Url. The URL is appended with .../SSO/login/Domain Name.
Identity Provider Login URL	This is a required field. You can enter the login URL of the Identity Provider
Identity Provider Logout URL	You can enter the Logout URL of the Identity Provider.
Identity Provider Certificate	This is a required field. It defines the Public Key of the Identity Provider. Once the Identity Provider Certificate is entered, the Server

	Name and Valid Until field are visible; these are read-only fields.

The Identity Provider Server and Nimsoft Service Desk have to be able to share metadata to establish trust and enable Single Sign On.

Once Single Sign on is configured, users can seamlessly log into Nimsoft Service Desk without having to log into the application again.

Inbound Email Configuration

Users can communicate with Nimsoft Service Desk by email; they can create and send a new email or respond to an email sent from the application. Nimsoft Service Desk can convert incoming emails into support requests or process existing request by updating them. Emails support HTML, as well as Plain/Text emails with attachments.

You can configure Inbound Emails from the Manage Configuration link under Application Setup. Click on Inbound Email tab open the form.

Mailbox Name	Associated Email	Server Name	User Name	Password	Leave	Email Processor Action
InfraDesk 5.0 Inbo...	ada1000@zinc.en...				No	ESD_processInc...
Slice#1000	Rajiv@engg.barod...				No	ESD_processInc...
Slice#1000	Sonia@engg.barod...				No	ESD_processInc...
Slice#1000	Sapana@engg.ba...				No	ESD_processInc...

Field	Explanation
Mailbox Name	This defines the name of the mailbox. Emails can be received in one or more pre-configured mailboxes.
Associated Email Address	This defines the email address for the mailbox.
Server Name	This defines the name of the email server.
User Name	This identifies the user who administers the email server.
Password	This identifies the password of the user who administers the email server.
Leave Messages on Server	You can choose either "Yes" or "No". If you choose "Yes", the email will remain stored in the email server even after the application has accessed the email. However, if you select "No",

	the email will get deleted from email server after the application has accessed it. Therefore, to ensure that the email is retained in its original form by the email server, you must select “Yes”.
Email Processor Action	This is the default action option for incoming emails.

The above fields need to be configured if the application is deployed on a Windows Server and the email action is going to be managed via an Exchange Server.

If your machine is deployed on a Linux machine, Sendmail will have to be configured for setting up email actions.

Outbound Email Configuration

Outbound Email tab allows you to configure aspects of the outbound emails. You can define the email recipient/s, format the email, block and redirect emails to specific recipients, define the hostname, etc.

You can configure Outbound Emails from the Manage Configuration link under Application Setup. Click on Outbound Email Configuration open the form.

The Outbound Email Configuration tab displays the following fields

Field	Explanation
Mailbox Function	This is a read only field that displays the function of the mailbox.
Slice	This is a read only field that displays the slice number.
Mailbox Profile Name	You can fill an appropriate mailbox profile name.
Status	The default status is Enabled. You can choose to make the status Disable and stop outgoing emails.

Email Server Name	You can fill an appropriate Email Server Name.
Email Server Username	You can fill an appropriate email server username.
Email Server Password	You can fill an appropriate email server password.
Default To Recipient	You can define the default recipient for the outgoing email(s).
Default CC Recipient	You can define the default CC recipient for the outgoing email(s).
Default BCC Recipient	You can define the default BCC recipient for the outgoing email(s).
Block Outgoing Emails	This drop-down option of “Yes” or “No” allows you to block the outbound email.
Redirect Email Address	Here you can specify the email id of the recipient other than the default recipient. If you block the outgoing email and leave the Status “Enabled”, you can redirect the email to a customized email recipient by entering the email id in this field. This will take the email to the redirected recipient instead of the default recipient.
HTML Template	This field allows you to use HTML script to format all outgoing emails. For example a Company letterhead with a logo image etc.
Email Server (Hostname)	This is a required field where the hostname is defined.
Reply To Display Name	This is a required field where the reply-to name is specified.
Reply to Address	This is a required field where the reply-to address is specified.

External Notifications

While bi-directional Email communications is built into the application, Nimsoft Service Desk can also be configured to allow External Notification like Phone Notification with services from an External Service Provider. This functionality can be used if the additional service is purchased from the Service Provider.

Currently, External Notifications can be configured to allow Phone Notification for SLA threshold violations, with the External Services being provided by MIR3.

You can configure the External Notifications from the External Notifications tab in the Manage Configuration form. Clicking on the form reveals the External Configurations form

The screenshot shows a configuration window with several tabs: General Information, Licenses, Single Sign On, Inbound Email, Outbound Email, External Notification, and Job Triggers. The 'External Notification' tab is active. It contains three main sections:

- Service Provider Details:** Includes a checkbox for 'Enable External Notification Configuration?' (checked), 'System Name' (MR3), 'Username' (Jagadish), 'Password' (masked), and 'System URL' (https://inwebservices.mr3.com/services/v1.2/mr3).
- Response Details:** Includes a 'Notification Failed Default Action' dropdown set to 'Notification Failure'.
- External Notification Form:** Includes a table with 'Response Options' and 'Associated Workflow Action' columns, with rows for 'Acknowledge', 'Decline', 'Escalate', and 'Resolved'.

The fields in this tab are explained below:

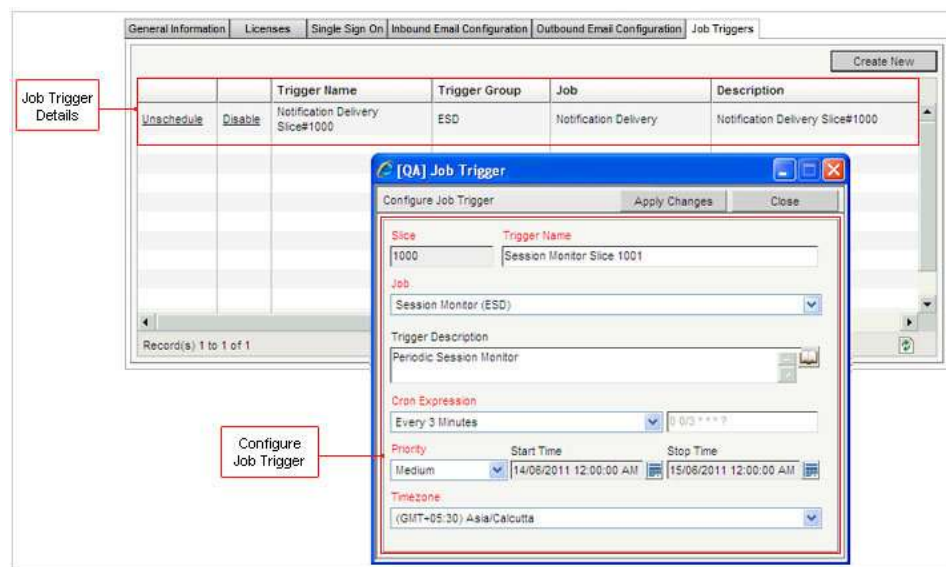
Field	Explanation
Enable External Notification Configurations	This checkbox controls whether the external notification configured is enabled or not. Checking on this checkbox raises the flag allowing the External Notification configurations to be recognized and used by the application.
System Name	This dropdown field allows you to select the External Notifications service provider. Currently the only options are None and MIR3. To enable Phone Notifications, select MIR3 in this field.
Username	In this field, you can enter the User Name provided to you by MIR3 when you subscribed for the External Notification service
Password	In this field, you can enter the Password provided to you by MIR3 when you subscribed for the External Notification service. Password is displayed in encrypted form on the UI.
System URL	In this field you can enter the access URL Provided by MIR 3 when you subscribed for the External Notification service.
Response Actions	This section allows you to enter details of Options for Actions delivered by MIR 3 and the corresponding Workflow Action to get executed when an option is selected.
Notification Failed Default Action	In this field, you can select a workflow action that will get executed if the phone notification from MIR3 to the intended recipient fails for any reason.
Response Options	In the five fields below, you can enter what options can be selected by a recipient who responds to a Phone Notification. When an SLA Phone Notification is triggered, the Options entered here will be read out after the notification message, as possible actions that can be taken on the ticket.
Associated Workflows	In the five fields below, you can enter a workflow action that will be executed when the corresponding Response Option is selected by a recipient of an SLA Phone Notification.

Based on the Response Options configured in the fields; and based on the response to options; a workflow action will get executed on the ticket; allowing the agents/analyst working on the ticket to take action on the ticket before a SLA is violated

Job Triggers

There are some tasks/ jobs taken up periodically by the application to enable the smooth functioning of the application. As an Application Administrator, you have the ability to configure and schedule some of these Job Triggers. Some of these are periodic while others get triggered by some action.

You can configure job triggers from the Manage Configuration link under Application Setup. Clicking on Job Triggers tab open the Form. To create a Job Trigger, click on the Create New action button. This will open the Configure Job Trigger look up.



The table below identifies the fields available on Configure Job Trigger look up.

Field	Explanation
Slice	This is a read-only field that displays the unique Slice ID.
Trigger Name	This is a required field in which you must enter an appropriate name for the Job Trigger.
Job	This is a required field. You must select an appropriate system defined job from the available drop down list.
Trigger Description	Here you can enter any information describing the Job Trigger.
Cron Expression	This is a required field. You must choose the frequency of Cron Job triggers from the options available in the drop down menu in minutes, hours, months, etc. You can also choose Custom Expression. If you opt for Custom Expression, the adjoining text field gets activated. Here you have to fill in the expression in

	code (such as: for every 3 minutes it is 0 0/3 * * *? or for every 5 minutes it is 0 0/5 * * *?). Cron jobs are periodic in nature and you can define how frequently they will be executed.
Priority	You can select the priority as appropriate by choosing an option from the drop-down options of Critical, High, Medium, and Low.
Start Time	You can select the date and time to schedule the Job Trigger.
Stop Time	You can select the date and time to stop the Job Trigger.
Time Zone	You can choose an appropriate time zone from the options available in the drop down list.
Apply Changes	You can click on this button to create the Job Trigger.

The table under Job Triggers tab will also display the following:

- **Unschedule:** This action link lets you delete a job.
- **Disable:** This action link lets you disable a job and again enable it, if required.
- **Enable:** This action link lets you enable a job trigger, when required.
- **Trigger Group:** At present all belong to the ESD Group.
- **Fire Next:** This specifies the date and time when the Job will be fired next.
- **Last Fired:** This specifies the date and time when the Job was last fired.
- **Status:** This is auto generated by the application based on the time and date scheduled for the Job Trigger.
- **Total Run Time:** This displays the total time of the running triggers from start to the present time or end time.

The Configure Job Trigger look up has Jobs available in a drop-down list. Given below is a brief description of these Jobs. You can choose the Job and enable them as per the organization needs.

Job	Action
Action Trigger (ESD)	Enables Action Scripts; however, it is not used now.
Auto Close Tickets (ESD)	Auto Closes a ticket after "x" number of days based on

	Workflow action setting a ticket to Resolved status.
Change Approval Background Process (ESD)	Performs background processes related to Change Approval workflow. Such as sending notifications to Approver / reviewers and applying "Approval Type" decision rule to responses received
Disk Cleanup (IAF)	Performs batch cleanup of temporary files from folders that are dedicated to store such files.
Generate Scheduled Report (ESD)	Process creation of scheduled reports and distribute it to the pre-defined recipients as an email attachment.
Message Receiver (ESD)	Receives email messages stored on a IMAP server that in turn can be processed by the Service Desk application for creation of new support cases based on the new support requests sent via email. (For Windows Operating system)
Notification Delivery (ESD)	Sends email notifications to appropriate recipients by polling the outbound email queue.
Polling Mailbox Provider (ESD)	Provides advanced polling-based processing semantics applied to IMAP mailboxes by forking out separate child jobs (for each mailbox associated with a tenant slice) that execute in parallel and process new messages.
Process Service Feedback Schedules (ESD)	Generates email notifications that must be sent to customers for all the active schedules for taking service feedback.
Relay Phone Messages	Sends or delivers messages to an individual destination or a "group" comprising of pre-defined set of destinations in the group simultaneously for acceptance or acknowledgement by the recipients
Track and Monitor Responses	Tracks responses provided after receiving a message by choosing an option from a pre-defined menu from a destination (device).
Scheduled Task Invoker (ESD)	Triggers the Scheduled Actions configured in Manage Schedules module as per the schedule details.
Service Level Compliance Monitoring (ESD)	Monitors whether measured service level performance metrics are in compliance with performance targets specified in SLAs.
Session Monitor (ESD)	Job to update last accessed URL and time for logged in users.
SQL Executor (ESD)	Executes a SQL DML Statement associated with the trigger firing this job against application database. For fulfilling additional needs of customer organization.

SQL Executor (IAF)	Executes a SQL DML Statement associated with the trigger firing this job against platform database. For fulfilling additional needs of customer organization.

Note: (IAF) is for Platform based Jobs. (ESD) is for application based Jobs.

Some of these Jobs will need to be Scheduled and/or Enabled after the slice has been provisioned. While most Jobs are already scheduled, by default they are in disabled state. You will need to Enable the background jobs to undertake the background jobs that they process. You can enable the job triggers by clicking on the Disable link in the table listing the Job Triggers.

Some Job Triggers like Relay Notification Job and Response Tracker Job will have to be manually scheduled if external notification action is being configured in your slice. The Relay Phone Messages and Track and Monitor Responses jobs are needed to poll for any SLA Target threshold rules with a Phone Notification action associated with it. When configuring these jobs, you will have to take due care to ensure that the time duration at which the job is scheduled to run (Cron Expression) is lesser than the lowest Threshold value.

For example, if the lowest threshold rule value is 10 minutes, the Job should have a Corn expression of 2 or 3 minutes to allow time for the notification to be relayed on time, and response to be received and appropriate workflow action to be applied to the ticket on time.

How Do I

Below are some actions you can take from the Manage Configuration form.

Manage Session Timeout

You can manage Session Timeout from the Session Timeout field under General Information tab of Manage Configuration.

To manage Session Timeout:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will open with pre-populated information in the form under General Information Tab.

Step 2: Enter the number of minutes in the field under Session Timeout.

This number will define the number of minutes the application remains idle before the server terminates it automatically. The default time is 60 minutes. You can choose to increase or decrease this time.

Step 3: Click on Apply Changes to apply the Session Timeout time.

The Session Timeout will get applied next time a user logs into the application.

Choose a Password Strength

Choosing a Password Strength allows you to define the complexity of password. It is a measure of the effectiveness of a password in resisting guessing and brute-force attacks.

To apply a Password Strength:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will open with pre-populated information in the form under General Information Tab.

Step 2: Choose a level from the options provided under Password Strength. You can choose between levels 1 to 4 to increase the complexity of password:

Level 1: Password must be at least 8 characters long

Level 2: Level 1 + Password must be a combination of upper and lower characters

Level 3: Level 2 + Password must contain at least one numeral

Level 4: Level 3 + Password must contain at least one special character

Step 3: Click on Apply Changes to apply the Password Strength.

Add or Renew Licenses

When Service Desk is installed, by default license of 30 days is associated with the Slice. Within these 30 days you must renew the licenses; otherwise, the system gets locked and becomes inaccessible.

When a valid license is about to expire, starting 7 days before expiry, the application displays an advance notice about the license expiry to Application administrators upon logging. When Service Desk Support team gets confirmation to issue new licenses to a customer, they send out the licenses to the customer via email. You can use the License Keys sent via mail to renew or add the licenses.

To add or renew licenses:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will be displayed.

Step 2: Click on the Licenses tab to display a list of licenses currently allotted to the slice.

Step 3: Paste the License Key(s) sent to you via email by Support in the License Key(s) field.

Step 4: Click on Add Licenses action button to renew or add licenses.

The information on the number of Web-Services, Self-Service, Fixed, and Floater licenses assigned, license validity period etc. will get populated in the table.

Block and Redirect Outbound Emails

Generally, outbound mails can be configured to reach the default recipient. However, in some situations, you may want to send emails to recipients other than the default recipient. Nimsoft Service Desk allows you to block all outgoing emails and redirect all outgoing emails to the recipient specified by you.

To block and redirect outbound emails to a specific recipient other than the default recipient:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will open.

Step 2: Click on the Outbound Mail Configuration tab.

The Outbound Mail Configuration form will be displayed.

Step 3: Fill in the required information, such as Email Server (Hostname), Reply-To Display Name, and Reply-To Address. Fill in any other information such as Mailbox Profile Name, Default To Recipient, Default CC Recipient, Default BCC Recipient, if required.

Step 4: Ensure that the Status field is "Enabled".

If you "Disable" this field the outgoing emails will not be sent out by the application.

Step 5: Choose option "Yes" from the drop-down list under Block Outgoing Emails.

This will ensure that the outgoing email is not sent to the Recipients, Cc, Bcc and Default Recipients.

Step 6: Specify the email ID of the person to whom you want send the email in the Redirect Email Address field.

This will ensure that the email is sent to the email address mention here instead of the default recipient.

Format Outbound Emails

Outbound Emails can be formatted to display a uniform look and feel (like display company branding, signature etc) before being sent. This ensures that all outgoing emails have a standard appearance and format.

To format outbound emails:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will open.

Step 2: Click on the Outbound Mail Configuration tab.

The Outbound Mail Configuration form will be displayed.

Step 3: Type in HTML script in the HTML Template field to define the format of all outgoing email.

This will ensure that outbound emails are formatted as specified.

Create a New Job Trigger

As an Application Administrator, you have the ability to configure and schedule Job Triggers for jobs taken up periodically by the application.

To create a new Job Trigger:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration form will open.

Step 2: Click on the Job Triggers tab to view the job triggers form.

A list of triggers that have been configured will be displayed. You can enable/disable an existing job trigger or unschedule the trigger by clicking on the link in the form.

To create a new trigger:

Step 3: Click on the Create New action button.

The Configure Job Trigger look up will open.

Step 4: Fill in an appropriate Trigger Name.

Step 5: In the Job field, click on the dropdown to view a list of available Jobs. Select the background job you wish to configure.

All background jobs are system defined. You can only choose from the list available.

Step 6: Select an appropriate Cron Expression to define the frequency at which you want the job to run. You can choose the Corn expression available in the dropdown list.

Step 7: Select the priority, as appropriate, by choosing an option from the drop-down options of Critical, High, Medium, and Low.

Step 8: If you want to configure the Job Trigger to run for a specific period, select the start and end date and time to schedule the Job Trigger. Leave the end time and date blank if you want the Job Trigger to run perpetually.

Step 9: Select the Time zone at which you want the job to run. You can choose from the available drop down list.

Step 10: Click on Apply Changes to create the Job Trigger.

The Job Trigger and its parameters will get displayed in the table under Job Triggers tab.

After the Job Trigger is configured; it will be displayed in the Job Triggers form. All new triggers are in disabled state. Click on the Enable Link to enable the trigger.

Frequently Asked Questions

Below are answers to some questions you may have related to managing Configurations.

What will get deleted if I execute Purge Transaction?

All tickets will get removed from the slice. This includes all related ticke or global tickets.

When would I need to execute Remap Imported CI Attributes?

If you have bulk uploaded additional CI Attributes into the slice, you will need to remaps these new CI attributes to existing CI attribute templates. Then, you will need to execute the Remap Imported CI Attribute Take Action option.

Can I create a Job Trigger for my own routine work?

Job Triggers are created for system defined jobs. You can see the list of jobs in the Configure Job Trigger lookup in the drop-down list under Jobs. If your routine work coincides with the system defined jobs, you can create a job trigger for it.

Chapter 9: Email Setup

Overview

Nimsoft Service Desk can be configured to allow emails that are sent to pre-configured email box(es), to create and modify tickets. The application can also be configured to enable notifications to be sent out directly from a ticket either by manual action or as automated notifications based on an auto-route or workflow action. Notifications can also get sent for Approval, Service Feedback and SLA escalations.

Self-Service users can send out a request to the help desk/support email ID, which will result in a ticket being logged in Nimsoft Service Desk. Based on any applicable auto-route or default routing rules; a ticket gets assigned to the appropriate support group and a notification is sent out about logging of the request. A ticket can be updated by replying to the notification received from the ticket.

Service Desk Agents can manually send out a mail from the ticket; or mark the worklog to be sent as an email to intended recipients. They can also schedule notifications to be sent out at a future date and time

This section explains the actions required to setup the Email functionality to enable incoming and outgoing email interactions with Nimsoft Service Desk. Details on the fields in the forms below are under [Manage Configurations](#) link in this guide.

Setting up Email Functionality

Once you have installed Nimsoft Service Desk; you will need to configure Inbound and Outbound Email function, configure required job triggers for background jobs related to emails and configure Communication Templates to allow notifications to be associated with ticket auto-routes and workflow actions, SLA escalations and Service Feedback schedules.

Some Email formats that are supported as acceptable Email Ids are:

username@varied.com,

username@varied.con,

username@varied.local, ...etc.

Inbound Email Configuration

Nimsoft Service Desk can convert incoming emails into support requests or process existing request by updating them. Emails formats supported are HTML, as well as Plain/Text emails with attachments. Prior to configuring the inbound email function you must have:

- One or more valid Email IDs; to which requesters will send a mail requesting for IT support.
- Email Exchange Server Name.
- Email Server User Name.
- Email Server Password.

You can configure Inbound Emails from the Manage Configurations form under Application Setup.

The list below provides information on the actions that can be configured or managed to fully exploit the email functionality.

Depending on the workflow or auto-routes you wish to establish you can:

- Configure multiple mailboxes related to your instance of Nimsoft Service Desk.
- Set the default Support Group to which tickets logged via email get routed.
- Configure workflow or auto-route matching conditions based on Sent To mail ID.
- Configure workflow or auto-route matching conditions based on email Subject.

The requestor's email Subject gets converted into the Ticket Description and the body of the mail gets populated in the Details field. Any attachment related to the email gets related to the ticket as an attachment.

If the incoming email is sent in response to a notification from a ticket and the Subject is unaltered and contains RE, Re or FW and the ticket number; the application recognizes the relation to an existing ticket and the email related to the open ticket and can be seen in the Activity Tab of the ticket.

If the first letter in the body of the reply to an approval notification is Approved or Rejected (or Approve or Reject), the Approval or Rejection gets related to the ticket and the status of the ticket gets modified accordingly.

Note: If the Subject of the reply to an email from the ticket is modified and does not contain Re, RE or FW AND the Ticket Number; the incoming mail will result in the creation of a new ticket.

Outbound Email Configuration

You can configure Nimsoft Service Desk to send out automatic notifications based on ticket workflow or auto-routes. Outbound notifications also go out in response to actions like Worklog entries (Client Facing worklogs), manual notifications from the ticket, Approval Notification, Service Feedback Schedule, SLA Escalations and Password Resetting.

Notifications are sent out to the contact's email ID set in the contact record. You can configure Outbound Emails from the Manage Configuration link under Application Setup.

The actions you can take related to outbound emails are:

- Enable or Disable Outbound emails
- Set Reply to Senders Display Name and ID
- Block and redirect emails to a specific mailbox.
- Format an HTML template for outgoing mails.

To configure outbound mails you need to enter valid Email Server Hostname and valid Reply to Name and Address. By formatting the HTML template, you can give a standard look and feel to the notifications sent out from the application.

The notifications that are sent out can be created and modified using the Manage Communication Template form under Workflow Actions in the application UI.

Configuring Job Triggers

To enable the application to perform tasks like sending and receiving emails, sending out service feedback schedules, monitoring SLA compliance, identifying and forwarding approval notifications etc., there are several background jobs that run in the backend. While some jobs are periodic, others get triggered by another related action.

You have to configure or enable job triggers to perform these background jobs. You can configure job triggers from the Manage Configuration form under Application Setup.

For customers having On-Premise installation of Nimsoft Service Desk, you have to configure and then enable a new job trigger "Polling Mailbox Provider", to enable the email functionality.

You can create this new trigger, in the Job Triggers tab on the Manage Configurations form. The tab will display a list of triggers already created. These triggers will be in Disabled state (with a button saying - Enable). You will have to enable all triggers for the background jobs to run.

To configure the Job Trigger:

- Click on Create New action button in the Manage Configurations form.

- Give the Job Trigger an appropriate name.
- From the dropdown list in the Job field, select the Job Trigger 'Polling Mailbox Provider'
- Add Description if needed
- Select Frequency at which your mail Exchange folder should be polled for new mails
- Choose whether mails should be retained in the mail server after they have been fetched by the application
- Click on Apply Changes to save the new Job Trigger.

The new trigger will be listed in the table in the Job Triggers tab. It will be in disabled state. Click on Enable to enable the job trigger.

For customers using Nimsoft Service Desk in the SaaS mode; the initial email configurations and configuration of the job triggers are completed during slice provisioning. You can take actions like adding additional email mailboxes to which mails can be sent.

Known Limitations and Workarounds

Emails sent in a Unicode language will result in ticket creation in the language in which the mail was sent. However, there are some limitations related to Unicode languages special characters and field length.

This section identifies the known limitations related to the sending and receiving emails from the application. The limitations are caused due to factors listed below:

- Special Characters like single quote, double quote, contiguous spaces, parenthesis, apostrophe, dollar character etc.
- XML reserved characters
- Double Byte characters
- Field length

The following factors may cause the email functionality to cause unexpected behavior:

- Emails with special XML characters (reserved characters)
- Emails in languages using Double Byte characters

- More than 512 characters in the To, CC or BCC fields of the email
- Details field (email body) having more than 4000 characters.

How Do I

Below are some actions you can take related to setting up Emails.

Block and redirect outbound emails

Generally, outbound mails can be configured to reach the default recipient. However, in some situations, you may want to send emails to recipients other than the default recipient. Nimsoft Service Desk allows you to block all outgoing emails and redirect all outgoing emails to the recipient specified by you.

To block and redirect outbound emails to a specific recipient other than the default recipient:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will open.

Step 2: Click on the Outbound Mail Configuration tab.

The Outbound Mail Configuration form will be displayed.

Step 3: Fill in the required information, such as Email Server (Hostname), Reply-To Display Name, and Reply-To Address. Fill in any other information such as Mailbox Profile Name, Default To Recipient, Default CC Recipient, Default BCC Recipient, if required.

Step 4: Ensure that the Status field is "Enabled".

If you "Disable" this field the outgoing emails will not be sent out by the application.

Step 5: Choose option "Yes" from the drop-down list under Block Outgoing Emails.

This will ensure that the outgoing email is not sent to the Recipients, Cc, Bcc and Default Recipients.

Step 6: Specify the email ID of the person to whom you want send the email in the Redirect Email Address field.

This will ensure that the email is sent to the email address mention here instead of the default recipient.

Format outbound emails

Outbound Emails can be formatted to display a uniform look and feel (like display company branding, signature etc.) before being sent. This ensures that all outgoing emails have a standard appearance and format.

To format outbound emails:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration maintenance form will open.

Step 2: Click on the Outbound Mail Configuration tab.

The Outbound Mail Configuration form will be displayed.

Step 3: Type in HTML script in the HTML Template field to define the format of all outgoing email.

This will ensure that outbound emails are formatted as specified.

Create a new job trigger

As an Application Administrator, you have the ability to configure and schedule Job Triggers for jobs taken up periodically by the application.

To create a new Job Trigger:

Step 1: Click on the Manage Configuration link in Application Setup.

The Manage Configuration form will open.

Step 2: Click on the Job Triggers tab to view the job triggers form.

A list of triggers that have been configured will be displayed. You can enable/disable an existing job trigger or Unschedule the trigger by clicking on the link in the form.

To create a new trigger:

Step 3: Click on the Create New action button.

The Configure Job Trigger look up will open.

Step 4: Fill in an appropriate Trigger Name.

Step 5: In the Job field, click on the dropdown to view a list of available Jobs. Select the background job you wish to configure.

All background jobs are system defined. You can only choose from the list available.

Step 6: Select an appropriate Cron Expression to define the frequency at which you want the job to run. You can choose the Corn expression available in the dropdown list.

Step 7: Select the priority, as appropriate, by choosing an option from the drop-down options of Critical, High, Medium, and Low.

Step 8: If you want to configure the Job Trigger to run for a specific period, select the start and end date and time to schedule the Job Trigger. Leave the end time and date blank if you want the Job Trigger to run perpetually.

Step 9: Select the Time zone at which you want the job to run. You can choose from the available drop down list.

Step 10: Click on Apply Changes to create the Job Trigger.

The Job Trigger and its parameters will get displayed in the table under Job Triggers tab.

After the Job Trigger is configured; it will be displayed in the Job Triggers form. All new triggers are in disabled state. Click on the Enable Link to enable the trigger.

Frequently Asked Questions

Some questions that you may have regarding Manage Configurations and Manage Communication Template are listed below:

What will get deleted if I execute Purge Transaction?

All tickets will get removed from the slice. This includes all related ticke or global tickets.

When would I need to execute Remap Imported CI Attributes?

If you have bulk uploaded additional CI Attributes into the slice, you will need to remaps these new CI attributes to existing CI attribute templates. Then, you will need to execute the Remap Imported CI Attribute Take Action option.

Can I create a Job Trigger for my own routine work?

Job Triggers are created for system defined jobs. You can see the list of jobs in the Configure Job Trigger lookup in the drop-down list under Jobs. If your routine work coincides with the system defined jobs, you can create a job trigger for it.

Chapter 10: Manage Organization

Overview

When a new instance of the application is created, the first sets of records that are created are records for Organization, Support Group, Contact, Roles and Configuration Items. Contacts and Support Groups and Configuration Items can be related to an Organization; and this relationship can be exploited if Organization Based Security is being enabled.

Various aspects related to creating and managing Organization records is explained in this section.

Manage Organizations

The Organization record within Nimsoft Service Desk can be configured at three hierarchical levels i.e. Organization, Sites related to the Organization, and Locations related to each Site.

While you have to configure an organization record, you can choose whether or not to define Site(s) under the Organization, and Location(s) related to a Site.

You can configure multiple organization records within your instance of Nimsoft Service Desk; with each organization having multiple sites and each site having multiple locations. Therefore, as per your business requirements, you can configure individual organization records for Service Users, Service Providers, Vendors, Channel Partners, etc.

The actions you can take related to Manage Organization are:

Create and Modify Organizations

You can manage organizations from the Manage Organization link under Application Setup. Clicking on this link displays the Manage Organization form with a list of all existing organizations in the list section. You can click on any organization record to view more details, which get populated in the Organization Details section below.

Application Setup (Manage Organizations)

List Filters

Organization List

ID	Name	Main Phone	Main Fax	Web URL	Address
1	Info Corporation	91-295-2311-594	91-295-2311-594	http://www.info.com	600, Goldsmith Complex R.C. Dutt Road, Mumbai
78	Trans World Packag...	646-789-2314	646-789-2317	http://www.trans.com	Floor 22, 208 Edgemoor Avenue, 148 Street, M...
100	DevTSM Corp.	781-237-3419		http://www.devtsm.com	99 Southampten street, Boston, MA, 02116, USA
105	CAD Solutions Provid...	646-789-2367		http://www.cadsol.com	11 Bethovan Street, New York, NY, 10030-112
106	Database Support Inc.	609-272-3394		http://www.dbi.com	John Adams Street, Sank City, NY, 53983, USA
107	Desktop Support Inc.	215-269-4339		http://www.dsinc.com	8 Ontario Street, Philadelphia, PA, 19134
129	B Apple Support Inc.	646-983-6733		http://www.bapple.com	94 Langdon Street, New York, New York, 10003
131	MJ Test Org			http://www.mjtest.com	414, Scherth Complex, Vadodra, Gujarat, 390

Record(s) 1 to 8 of 8

Organization #79: Trans World Packaging Services Inc.

Terminate Apply Changes Create New Delete

Organization Details

Organization Name: Trans World Packaging Service Organization Type: -- Clear -- Web URL: <http://www.trans.com> Status: Active

Street Address: Floor # 22, 208 Edgemoor Ave City: New York State: NY Zip Code: 10030-1120

Main Phone: 646-789-2314 Main Fax: 646-789-2317 Country: USA

Organization Details | Location Information | Special Notes | Attachments | Contacts | Groups | Dependent Data

Recaller Name: Info Corporation Account Manager: John, Alisha ☐ Disable Service Feedbacks

Support Note: Support Phone: Support Email:

Image Name: Image Description:

You can modify details of the organization; and all records where the organization record is used get updated accordingly.

You can create a new organization record by providing the minimum required information i.e. Organization Name; and any other information like phone, website, etc. Once you Apply Changes to save the record, a new Organization record is created and additional tabs of Location Information, Special Notes, Attachments, Contacts Groups and Dependant Data are displayed along with the Organization Details section.

Making an Organization Inactive results in all related Sites and locations becoming inactive. When an organization is made inactive, those contacts records where the inactive Organization is marked as the Primary Organization, also become inactive; and these contacts will not be able to access the application.

Note: Please ensure that you don't make all organizations Inactive as that would lock out all users from the application.

You can also Terminate an Organization, if required, and thereby terminate all entities like Sites, locations, Contacts and Configuration Items that are related to the Organization.

However, removal of an organization from the application is based on data dependencies and existing relationships, which can be viewed in the Dependent Data tab of the Organization Record.

Create and Modify Site and Location

You can manage Site and Location details from the Location Information Tab. This tab displays a list of any Site and Location already associated with the Organization.

The screenshot shows the 'Location Information' tab with two sub-sections: 'Site Details' and 'Location Details'. The 'Site Details' section contains a table with columns: Site Name, Address, City, State, and Zip Code. The 'Location Details' section contains a table with columns: Building, Floor, Suite, Cube, and Closet. Both tables have 'Delete' and 'Edit' buttons for each row. The 'Site Details' table shows 5 records, and the 'Location Details' table shows 1 record.

		Site Name	Address	City	State	Zip Code
Delete	Edit	TMPS World HQ	Floor 22, 208, Edgecomb Avenue, 14...	New York	NY	10030-1120
Delete	Edit	TMPS US HQ	Floor 19-20, 208, Edgecomb Avenue...	New York	NY	10030-1120
Delete	Edit	Boston RO	410, Adams Street	Boston	MASS	02100
Delete	Edit	Hartford MO	93, Barryford Blvd.	Hartford	CT	06101
Delete	Edit	Charlotte Mto Plant	311, North Brooks Street	Charlotte	NC	28202

Record(s) 1 to 5 of 18

		Building	Floor	Suite	Cube	Closet
Delete	Edit	Orion Heights	10	SA		

Record(s) 1 to 1 of 1

You can add new Site(s) and/or Location(s); modify details of an existing Site or Location or manage the Status of a Site or Location (active or inactive). You have to add a Site before adding its Location details as the Location is related to a given Site. All the new Site(s) or Location(s) that are added get displayed in the table below.

Add Special Notes

If you wish to add any special comments about an organization, for example, information on any ongoing contracts or some critical factors, you can add a note in the Special Notes section. All notes that are added get listed in the table. You can edit or delete a note from within this tab.

Relate Attachment

You can relate an attachment to the organization record to provide additional information that is not captured in the other fields. You can choose from existing attachments (Global Attachments) or choose an attachment specific to the organization record.

Relate Contacts

You can manage contacts related to the organization from the Contacts tab. A list of contacts related to the organization can be seen in the table. You can relate new contacts to the Organization using the Relate Contacts action button.

To relate a contact, you can select the contact(s) to relate, specify a Relationship Type by selecting an appropriate option from a pre-configured drop-down list and relate the contact to the Organization.

You can unrelate a contact that has been related to the organization.

Note: When an organization is made Inactive, all contacts related to this Organization as Primary Organization will automatically become inactive. When an organization is terminated, all contacts related to the organization as Primary Organization will automatically be removed.

Relate Groups

You can relate Support Groups to an Organization from the Groups tab. Relating Support Groups to the Organization helps when enabling Organization Based Security. You can use the Relate Groups action button to view and locate Support Groups to the organization.

While you can choose to relate an Organization as a Primary Organization for a Support Group; it is not necessary to set a Primary Organization for the Support Group.

When an Organization is made inactive or deleted, the relationship with the Support Group gets removed; but the Support Group record remains intact.

View Dependent Data

You can choose to terminate an Organization, and thus terminate all records related to the Organization. When an organization is terminated, all contacts related to the organization as Primary Organization will automatically be removed.

Successful termination of the Organization and related records is possible only when all dependant data relationships are removed or the dependant data can be terminated with the Organization (depending on the nature of the record).

You can see details of related records and other data that could cause the Terminate Organization action to fail in the Dependent Data tab of the Organization record.

Before executing the Terminate Organization action, you must review the dependent Data. If any data from the dependent data group (Tickets, Sites, Locations, Contacts, CIs) is to be retained, it must be unrelated from the Organization. Also, transaction data, like workflow actions and auto-routes have to be unlinked from the organization before successfully terminating the organization record.

For CIs and Contacts that should get deleted when the Organization is Terminated, their dependent data links also need to be unlinked.

Any entity attached to a terminated data also gets removed from the application.

Manage Organization Check points

Some check-points to bear in mind when managing Organization records are:

- One instance can have multiple Organization records in your instance of the application
- Site and Location details can be configured only after configuring Organization Record
- Participation of contacts in Service Feedback can be controlled at the Organization Level
- All site(s) and location(s) related to an Organization become inactive if Organization is made Inactive.
- Contacts related to the organization become inactive when the Organization is made Inactive if the inactive organization is the Primary Organization for the contact
- Sites, Location, and Contacts have to be manually made active if an inactive Organization is made Active.
- When an organization is terminated, all transactions and Dependent Data also get deleted. You can see a list of dependent entities in the Dependent Data tab.
- When an Organization record is terminated, Support Group(s) related to the Organization remain intact. Only relationship with the Organization is removed.
- If Organization Based Security is enabled, contacts will need to be related to an organization in order to view tickets and configuration items related to that organization.

How Do I

Below are some actions you can take related to managing Organizations.

Create and Manage Organization record

You can configure multiple Organization records in your instance of the application. You can also modify an existing Organization record as per need.

To manage existing organization records, and create new Organization record:

Step 1: Click on the Manage Organization link under Application Setup. A List of all existing organizations will be displayed.

You can view an organization record, modify an existing record or Create new record in the form below.

Step 2: Click on the Create New action button to create a new organization record.

Step 3: Enter a Name for the Organization, which is a required field to save the organization record.

Step 4: Enter other required information such as phone number, Web URL, address, etc. as appropriate.

Step 5: In the Organization section, you can select a Reseller name, Account Manager, etc. If the Organization is a Support Organization, you can also add details like Support Phone, Support Email id etc.

Step 6: You can choose to exclude this Organization and contacts related to this organization from the Service Feedback process. To do so, check the Disable Service Feedback checkbox.

You may choose to leave this section blank if this information is not relevant for the context in which the organization record will get used.

Step 6: Click on Apply Changes to save the new Organization record.

Once the Organization record is created, other tabs for Location Information, Special Notes, Attachments, Contacts, Groups and Dependant Data tabs get displayed.

You can create Site and Location for an Organization in the Location Information tab. You can create a location only after configuring a Site.

Step 7: To create a Site, click the Add Site action button.

The Organization Site lookup will be displayed. Enter required information about the site like Site Name, Address etc. Depending on the Country and time-zone for the Site, you can choose an appropriate Time-Zone from the dropdown list.

Click Apply Change to save the Site details.

After configuring the Site, you can add Location Details using the Add Location action button.

Step 8: (Optional) To add any special information about the Organization like Contract details etc., click on the Special Notes tab.

Step 9: (Optional) To relate an Attachment to the Organization record if needed, click on the Attachment Tab. You can either add an Existing Attachment (already uploaded to the application) or add a new Attachment from a different location.

Step 10: To relate Contacts to the Organization, click on the Contacts tab. Click on the Add Contacts action button to view the Name Search Lookup.

In the Name Search lookup, you can search for Contacts you wish to relate to the Organization. You have to add Relationship type before you relate a contact to the Organization.

You can unrelate a Contact by clicking on Unrelate.

Step 11: To relate Support Groups to the Organization, click the Groups tab. Click on Relate Groups action button to view the Name Search lookup.

In the Name Search lookup, you can search for Support Groups that you wish to relate to the Organization. You have to add Relationship Type before related the Support Group to the Organization. You can choose to set the Organization as Primary for the Support Group.

You can unrelate a Support Group by clicking on Unrelate.

Note: Organization records can be bulk uploaded into application during the initial set up phase.

If you check on the Disable Service Feedback, the organization will not be displayed in participating organizations list when configuring Service Feedback Schedules. Contacts with this organization as Primary Organization will also be excluded from the Service Feedback process.

Create Site and Location for an Organization

An organization can have multiple sites and a site can have multiple locations. You can create Site and Location information for an Organization from within the Organization record.

To create and manage Site and Location for an Organization:

Step 1: Click on the Manage Organization link under Application Setup. The List of all existing organizations will be displayed. From the list, choose the Organization for which you wish to configure Site and Location details.

When an Organization record is saved, Location Information and other tabs get displayed in the form.

Step 2: Click on the Location Information tab.

Any existing sites related to the organization will be listed in the table below. You can add Sites to the Organization in the form below.

Step 3: Click on the Add Site button. The Organization Site lookup will be displayed.

Step 4: Fill in the mandatory information on Site Name, Street Address, Country, State, City, and Zip Code.

You can fill in the additional fields like Country Code, State Code and Building; however, these fields are not mandatory.

Step 5: You can define an ID for the Site if needed. The Site ID does not get generated by default.

Step 6: Select a Time Zone for the site. You can set the Site Time-Zone as different from the default Slice Time-Zone.

Step 7: Click on Apply Changes. The Lookup will close and the Site information will get added to the Organization record form.

You can now configure an Location under the site. When you click on the Site listing in the table, the Location Tab will get enabled.

Step 8: Click on Add Location button. The Location lookup will get displayed.

Step 9: Enter the Building Name, which is a required field. You can add other details like Floor, Suite, etc.

Step 10: Click on Apply Changes. The lookup will close and the Location information will get added to the list.

Note: You can add a Location only after the relevant Site record is created.

While Time Zone is not a mandatory field, you can set the time-zone for a Site to either the different from that of organization or the slice. If no Time-Zone is set; default slice time-zone set in the Config Parameters gets applied to the site.

Terminate an Organization

You can terminate an organization and remove all transaction and dependent data.

To remove the organization record from the application:

Step 1: Click on the Manage Organization link under Application Setup. From the list, select the Organization for which you wish to remove.

The details of the organization will get populated in the form below.

Step 2: Click on the Dependent Data tab.

All records that are related to the organization will be displayed in this tab. This tab list information like the record name, description and Action on termination.

For some records, the Action on Termination will display “Delete will fail if dependent data is found”. For all such records, you will have to manually unrelate the record before terminating the organization.

For some records, the Action on Termination states that “All Dependent records will be deleted”. If you wish to retain any records related to these records; you will need to drill down to the details and manually unrelate the records you wish to retain.

Step 3: Manually unrelate the entity from the organization that need to be retained or dependent data that needs to be deleted in order to unrelated for the termination to succeed.

Step 4: Refresh the Information on “Dependent Data “ tab after manual action to verify that no dependent entities that needs to be retained, remains in the list.

Step 5: Click the “Terminate” action button when no dependent data remain for the Organization.

A Confirmation message; seeking confirmation of the action to Terminate Data is displayed. You can cancel the action or confirm the action. Upon confirmation of Termination, the Transaction data for the Organization and all related records get terminated.

Note: When an Organization record is Terminated, the Support Group related to the Organization remains intact. Only relationship between that Organization and the Support Group is removed.

Frequently Asked Questions

As Administrators, you may have many questions related to Organization, Site, or Location records. Given below is a list of FAQs related to Organization, Site, or Location records.

Can the same site have two locations with same Building Name?

Yes, a site can have more than one location with the same Building Name. However, it is advisable to add distinguishing mark in Location name so that users do not get confused while using a look up.

What happens when I click on Disable Service Feedback for an Organization; but do not check the flag for a site or location?

When you check the Disable Service Feedback for an organization, all contacts related to the Organization (and site or location related to the organization) as Primary Organization will not be included in the service feedback process.

The organization will not be available when selecting participating Organizations in a Feedback Schedule in the service feedback surveys.

Where can a User other than administrator view the information of Support note, Support Phone, and Support E mail for an Organization?

Self-Service users do not have access to details like Support Note, Support Phone, and Support Email for the organization on the application interface.

Service Desk agents can access these details under the Home Section of the application, in a link called Support Information. However, access to this link can be enabled or disabled by managing permissions to contacts, support groups, and roles.

What is the function of the Special Notes Tab? What sort of details can I record there?

The special notes tab allows you to provide additional information that can be classified as important or critical for a company. This tab allows you to capture any information that you think is useful to know about the organization. Any details in a text or alpha numeric values can be captured here.

It allows capturing relationship state as Excellent, Fair, Good, etc., and this information may help Agents to interact and communicate more effectively

For example, if you have a fixed duration contract with a vendor organization which has to be renewed by a given time, this information can be captured in the Special Notes section.

Will an attachment I relate to an organization be automatically available to all contacts of that organization?

No, an attachment does not become available to the organization by default. You can designate an attachment as Global Attachment, whereby the attachment becomes available for all relevant records across the application.

The Attachment is then available for all users of the slice, not just the users of that organization.

Can I terminate (delete) an Organization from the application if required?

Yes, you can terminate or remove an Organization from the application via Manage Organization in Application Setup. (For details, refer to How Do I - Terminate an organization record from the application)

Can I terminate an organization, but retain some of the dependent entities that are required?

Yes, before deleting the Organization, you will have to unrelate or delink such data from the organization. You can trace using the Dependent Data tab, all such entities that will get deleted. Once identified, you can manually unrelate the data. (For details, refer to How Do I - Terminate an organization record from the application).

Chapter 11: Manage Contacts

Overview

A contact refers to any person in the IT support process that interacts with the application either as a user of the service or provider of the service. A contact could be an End User who does not have access to Nimsoft Service Desk application; but is involved in the IT support process in one way or another. This could be a requester, vendor, service provider, or any other role providing or consuming IT Services.

Contacts can be independent entities within the application records; they can be grouped together into Support Groups; and contacts and groups can be clubbed together into a Role.

You can assign Permissions to Support Group or Role, and thereby to all contacts related to the Support Group or Role. This removes the need to assign Permissions individually to each contact being assigned the permission.

A contact can be associated with multiple organizations; though only one Organization is set as Primary Organization for the contact. If the Primary Organization is made inactive; the contact record automatically becomes inactive.

A contact can be made part of multiple support groups, associated with multiple roles, and be granted permissions for all actions related to the support group or role.

The different actions you can take related to Contact Records are explained below.

Create and Modify Contact Records

You can manage Contact records from the Manage Contacts link under Application Setup. Clicking on this link displays the Manage Contact Form.

Application Setup (Manage Contacts)

Contact List

ID	Full Name	Phone Details	Phone Number	Email	Job Title
55	Len, Timothy	Business	+1 312-557-1234	VP@len.com	VP marketing US-EU
56	Laluka, Anthony	Business	+1 312-557-1234	VP@laluka.com	VP Mfg.
57	Kerst, Vincent	Company	+44 020-326-6987	SSU14@kerst.com	CM-UK
58	Schulte, Daniel ITCM	Business	+49 765-907-0097	ITCM@schulte.com	IT Change Manager

Contact Profile

Title: Mr. John R. Beucus
 First Name: John
 Middle Name: R.
 Last Name: Beucus
 Email: J@beucus.com
 Office Code: 0001
 Pin #: 12345
 Time Zone: (GMT-05:00) America/New_York
 Locale: English (United States)
 Date Format: 12/19/2011 02:34:58 AM
 Language: English
 Status: Active

Contact Details

Employee ID: 12345
 External ID: 67890
 Notification Mechanism: Clear
 Pager Type: Text
 Pager Email Address: J@beucus.com
 Manager: Manager
 Business Segment: Business Segment
 Head Quarters: Head Quarters
 HR Generated: HR Generated
 Contractor: Contractor
 Start Date: 12/19/2011
 End Date: 12/19/2011

Out-of-Office

As the number of contact records is usually large, the table is not automatically populated. You can either search for a specific contact using the Contact's first or last name or enter search without specifying any criteria. You can also choose for filter the list using the available options.

The List Contacts table lists contact records stored in your instance of the application. You can click on a particular contact record to view more details.

You can modify details related to the contact and update the contact record. The modified details become available on all entities where the Contact is associated.

You can also view a list of open tickets logged by a contact in the Open Items tab and access the ticket directly from the contact record.

You can create a new contact record by specifying the minimum required information i.e. the First Name and Last Name of the contact and any other details like email, phone, and other contact details you wish to add and then save to create a new contact record.

Key factors to consider when creating or managing contacts are:

Enable Access

When creating a contact, you can specify whether the contact will be able to access Nimsoft Service Desk or not. If you wish to enable access, you have to check on the Enable Login checkbox and specify a System User ID for the contact.

Set Contact Locale

You can select a Locale for the contact; and enable the contact to use Nimsoft Service Desk in the language of the selected locale. You can choose from the dropdown options available.

When the contact logs in to the application, the application UI and other actions for which you have provided translations, will be displayed in language of the locale. If the contact wants, he/she can change the locale preference upon logging in.

VIP Contact

You can also mark a contact as **VIP Contact** if requests from this contact are to be prioritized differently. Other actions you can take are assigning a PIN to the contact, which will allow for contact authentication.

Designate Deputy

You can specify a **Deputy** or **Alternate Contact** for a contact. The chosen Deputy takes up the tasks assigned to the contact when the contact is not available. The Deputy has to be a member of at least one Organization-Site-Location and one group as the contact.

For this purpose the level at which contact is associated with an organization hierarchy and all level below are considered. For example, if the user belongs to a specific Site, other contacts of the site and all locations below the site are considered. Specifying a Deputy in the **Contact Records** helps as the contact does not need to choose a Deputy each time he raises the Out of Office flag.

Once the contact record is saved; additional tabs of Location, Open Items, Application, Special Notes, Attachments, and Related CIs are displayed. You can view and add relevant details from each tab.

Add Location Details

Once a contact record is saved, you can relate the contact to an organization and further specify site and location below the organization if you want to relate the contact to a specific site and/or location.

The **Add Location** action button displays a form where you can choose the relationship type from a pre-configured dropdown list and select an organization from the existing Organization records. Both these fields are mandatory. You can further choose site and location for the contact as appropriate.

You can view a list of organizations that the contact is related to in the Location Tab. You can relate multiple organizations to a contact record; however, you will have to specify any one organization as **Primary Organization**.

The system by default takes the first organization related to the slice as Primary Organization. You can set any other Organization as Primary and unrelate an organization from within this tab.

Manage Application Related Information

The Application tab of the contact record contains the contact's System User ID , License Type, and information on Support Group(s) that the contact is associated with. You can associate the contact to one or more Support Groups from this tab.

The actions you take in this tab are:

Assign System User ID

You can assign a System User ID for the contact from within this tab, if you have not set the contact's Email ID to be used as the default System User ID. You can set the Email ID as the Default user ID by setting the Configuration Parameter `DEFAULT_USER_ID_TO_EMAIL_ADDRESS` to Yes.

Assign License Type

A user with System User ID has to be assigned an appropriate License Type - Self-Service, Floater , Fixed or Web-Services. If a contact is assigned Self-Service License, he/she gets access to the Self-Service User Interface. A contact can be given only one license type, though you can change the License Type at any later stage.

Disable Service Feedback

You can enable or disable the contact's ability to participate in the Service Feedback process by checking or unchecking the Disable Service Feedback checkbox. However; a contact cannot participate in the Service Feedback process if the Disable Service Feedback flag is checked for the Primary Organization of the contact; even if at the contact level the flag is unchecked.

Relate Support Groups

You can manage Support Groups and Roles that the contact is part of. The table lists all Support Groups or Roles that the contact is related to. You can add new support groups or Roles from the Add Roles/Groups action button. A contact can be part of multiple support groups; however, only one group will be marked as Primary Group. You can change the Primary Group of the contact from within this tab.

Additional Information Tabs

The other information tabs in the contact record are Open Items, Special Notes, Attachments, and Related CI tabs.

View Open Items

In the Open Items tab, you can view a list of all Open tickets related to the contact as ticket requester (or requested for) or ticket owner (Assigned to Individual). The table lists all open tickets. You can view ticket details by clicking on the Edit option. The ticket opens in a new window, and you can modify the tickets, if required.

Add Special Notes

If you want to provide specific information about a contact, you can add special notes or comments to a contact record.

Relate Attachment

You can upload or remove an attachment from the Attachment tab. An attachment can be marked as Global, and be made available to all records like CI records, tickets, Knowledge Articles etc.

View Related CI

The Related CI tab lists all Configuration Items related to the Contact where the contact is the user, owner, or related to the CI in any other pre-defined way. However, you cannot relate or unrelate a CI from this tab.

View Dependent Data

The Dependent Data tab displays a list of dependent entities, their description, the action on termination, and the “Number of records” for each. This information is important if the Contact has to be unrelated manually before its associated organization is terminated.

Manage Contact Checkpoints

Some points to consider when managing contacts are:

- Login has to be enabled, for a contact to be able to access the application
- A contact with login enabled has to be assigned a license type
- A contact can be marked as VIP Users , if required

- A contact can be assigned PIN for authentication, if needed
- A contact's participation in the Service Feedback process can be enabled or disabled
- A contact can be related to multiple organizations; but one organization is defined as Primary Organization
- A contact can be related to multiple Support Groups but one group is defined as Primary Group
- A contact can be related to multiple Roles.

Note: If contact's time zone is not specified when the contact record is created or updated, then by default the contact's time-zone will be set as per the time-zone specified in the Config Parameter value DEFAULT_PARAMETER.

How Do I

Below are some actions you can take related to Managing Contacts.

Create and Manage Contact Records

You can create Contact records from the Manage Contacts link under Application Setup.

To create and manage Contact Records:

Step 1: Click on the Manage Contacts link under Application Setup. The manage contacts list and form will be displayed.

You can modify an existing contact or create a new contact in the form below.

Step 4: Click on Create New button to create a new contact record.

Step 5: Enter the First Name and Last Name of the contact. Both fields are required fields.

You can choose to fill in additional details like Title, Email ID, job title etc. However, these fields are not mandatory. You can choose to leave it as blank.

Step 6: Set a time-zone for the contact. This can be different from the time-zone associated with the Organization or Site.

Step 7: Set the locale preference for the new contact record. You can set a locale option different from that of the slice default.

Step 8: You can mark a Contact as VIP User, and if Login is to be enabled, you have to check the Enable Login checkbox for the contact.

Step 9: Provide contact details like Phone and Fax numbers for the Contact. You can choose not to provide this details as these fields are not mandatory. You can also associate a Deputy for the contact. This information is useful if the contact sets the Out of Office flag.

Step 10: Click on Apply Change to save the Contact record.

When the Contact Record is saved the other tabs of Location, Open Items, Application, Special Notes, Attachments and Related CI will get displayed on the form.

Step 11: Click on the Location tab. In this tab you can relate the contact to Organization, Site and Location (as required).

You can relate the contact to multiple organizations and set any one organization as Primary Organization.

In the Application Tab, you can assign the Contact a License and System User ID, relate the contact to Support Group/Roles, etc.

Step 12: If the Enable Login checkbox is checked, provide a System User ID for the contact and assign a License Type. This will control how the contact access and interacts with the application.

Step 13: You can check the Disable Service Feedback checkbox if you don't want the contact to participate in the Service Feedback process.

Step 14: To relate the contact to Support Group or Roles, click on the Add Roles/Groups button. Relate multiple groups or roles from the lookup. You have to set any one Group as Primary Group.

Step 15: Click on Special Notes Tab to add specific information about a contact.

Step 16: Click on Attachment - to upload any attachment.

Any Configuration Items related to the Contact will be displayed in the Related CI tab.

Note: When Contact records are created by the Contact Sync Utility; directly from your Directory server; the contact is by default assigned Self-Service License; with Self-Service as Primary Group. This will need to be modified subsequently and the contacts will need to be assigned an appropriate license type as needed.

Relate Contact to Organization, Site and Location

You can relate Contacts to Organization, Site and Location either from the Contact Record or from the Organization record. To relate Contact to Organization from the Contact Record:

Step 1: Click on the Manage Contacts link under Application Setup.

Step 2: Search for the Contact Record you wish to relate Organization to, either by searching by entering contact name, or from the list of all contact records.

Step 3: Click on the Contact record in the list to view details of the contact record in the form below.

Step 4: Click on the Location tab to view details of any Organization, Site or Location already related to the contact.

Step 5: Click on the Add Location to view the Contact Location lookup.

Step 6: Select the relationship type from the drop down list.

Step 7: Select an organization from the existing Organization records.

Step 8: You can also choose a Site related to the Organization and Location related to the site if required.

Step 9: Click on Apply Changes to save the changes and close the lookup.

The newly added Organizations, Sites and Location will be displayed as a list under the Location tab.

You can associate a contact with multiple organizations. However, one organization will have to be identified as the Primary organization for the contact.

You have to select Site before selecting Location. The list of Sites depends on the Organization selected and the list of Locations depends on the Site selected.

Frequently Asked Questions

Below are answers to some questions you may have related to managing Contacts.

What do I see some system defined contacts? Why are they needed?

The system defined contacts are the Notification Engine, Routing Engine, SLA Monitors, and other utilities that interact with the application to automate certain actions.

These entities are configured as System Defined contacts so that they are able to interact with the application to carry out their functions. You can find out whether a notification or assignment action was performed by the system or performed manually from the Activity tab records in a ticket.

Will all contacts configured in my instance on the application be able to access Nimsoft Service Desk?

No; all contacts configured in the application need not be given access to the application. For a contact to access the application, the login has to be enabled and the contact has to be assigned a System User ID.

Can a contact be associated with more than one organization, site or location?

Yes; a contact can be associated with multiple organizations, sites, and/or locations. A contact can also be located to multiple sites of the same organization. However, only one organization can be marked as Primary Organization of the contact.

If you do not manually set an Organization as Primary, the first Organization that the contact is related to becomes the default Primary Organization.

Can a contact belong to two locations but for different Organizations?

Yes, a contact can belong to two or more locations of different organizations. A contact can be related to multiple organizations, multiple sites, and multiple locations.

Can a contact be created and associated only with the organization, and not a site or location?

Yes; you can relate a contact only to an organization and decide not to relate to contact to a site or location. In such a case, making a site or location inactive will not affect the contact.

Can a Self-Service User view tickets logged by contacts from across different sites and locations?

If you have enabled the ability for Self-Service Users to view Organization Tickets, the Self-Service Users can view tickets logged by others belonging to the same Primary Organization. However, if the Primary Organization has Site and Location defined, then the user can view tickets by others with same Organization, Site, and Location as the logged in Self-Service User.

Only if the Primary Organization of the Self-Service User has just Organization (not site and Location) configured, the user will be able to view tickets logged by all contacts related to all sites and locations related to that Organization.

Can a contact be associated with a time zone that is different from the time-zone of the Organization/Site/Location he/she is related to?

Yes. A contact can be assigned a specific time zone that is different from the time zone of the site.

If you do not want to specify a time zone, application will ask you if you want to default to Site time zone for the contact.

A time zone is associated with the organization at the Slice Configuration level. A site can have a time zone different from the slice time-zone. A contact can have a time zone different from the Site time zone. The Contact time zone does not default to Site or Org time zone.

The first time zone in the Look up GMT+00.00 Africa/Abidjan becomes the default if one is not careful and changes it to what one really wants.

Can a contact record exist, but not be associated with any group? How does this impact the contact's ability to interact with Nimsoft Service Desk Application?

Yes; a contact does not necessarily need to be associated with a support group. By default, all contacts who are assigned Self-Service User license become members of the self-service group. Contacts who are assigned fixed or floater license become members of Public group.

Hence, not associating the contact with a support group does not in any explicit way change the way the contact interacts with Nimsoft Service Desk.

Can a contact who is a Self-Service User be associated with multiple groups?

Yes; a contact who is a Self-Service User can be associated with multiple groups. For example; the self-service user could be made member of a CAB or some other group. However, the primary group remains Self-Service Group. So, the contact can do only those actions which are allowed for a self-Service User through the Self Service user interface.

Does a user who is assigned to Self-service group with a self-service license, when assigned to another group, lose the membership of the Self Service Group?

No. The primary group of the Self-Service User remains as Self-Service Group as long as the license associated is a Self-Service User license. This group cannot be removed or changed till the license type is changed.

Do VIP Users have special permissions or access to some additional functionality?

No; VIP Users do not have any special permissions or access as access and permissions are controlled at contact, support group or role level. Flagging a contact as VIP user is only a way of highlighting that the user requests need to be prioritized differently by the support group working on the request.

Can I modify details related to the contact, like the contact first and last name? Will changes get reflected in other records and transactions?

Yes; you can modify all records for a contact. Modifying the records results in the change getting reflected in all existing records where the contact details appear (including tickets, CI records, etc.)

What happens when I make a contact inactive?

When a contact is made inactive, the contact will not be able to access the application. Also an inactive contact name will not show up on any name search (look up) across the application and hence cannot be associated with any new records in the application.

Can an inactive contact log into Nimsoft Service Desk application?

No; when a contact is made inactive, the system does not allow the contact to log in and transact with the application.

What happens when the deactivated Contact record is activated again?

When an inactive contact is activated again, the contact can access the application (if he/she has a User ID) and can interact with the application as any other active contact record.

Do I need to specify contact User ID and Password manually?

You do not have to manually specify System User ID if you set the Slice Configuration Parameter to use Email ID as default system user id. Otherwise, you will need to manually specify a user id.

As administrator, you can reset user password either from the contact record or from the Reset Password link. The action Reset Password results in a system generated password which gets automatically sent to the user by email. If a Contact does not have an Email address, application does not permit Change Password / Reset Password action to admin for that contact.

Can I reset the password for the user who does not have email ID or access to the email?

If you reset the password to generate a system generated password, the only way the changed password gets transmitted is via email. Hence resetting the password of a contact that does not have access to email is not permitted.

Is there any character limit for length of password?

Yes; there is a maximum password length of 25 characters.

Can I create multiple user records with the same user first name and last name? If yes, what could be the impact?

Yes, there can be more than one contact record with the same First Name and Last Name. The application does not enforce unique values in these fields. However, to avoid confusion, it is advisable to add some distinction to names so as to enable users (particularly Service Desk Agents) to distinguish the two contacts when using the contact record for other transactions in the application.

Can Contacts - SSU and Agents- modify their own contact records?

Contacts can modify some aspects of their contact records, like adding a new phone, changing an existing phone, etc. This can be done by the My Profile option available to both Self-Service Users and Service Desk Agents.

Chapter 12: Manage Support Group

Overview

A Support Group is a collection of contacts who are grouped together on the basis of specialization or functional expertise, role in the IT Support activities or geographical location of the Support Group.

Grouping of contacts into Support Groups helps particularly in managing the support tickets that are logged. Support Groups can be related to an Organization, and thus all contacts of that Support Group get related to an Organization. This can be used to enable Organization based security to control access to tickets and configuration items.

Auto-Routes can be configured for ticket assignment to a group and any member from the group can accept ownership of the ticket and work towards resolving it. This greatly reduces dependency on an Individual, thus, enhance the quality and time to respond to a ticket.

Relating contacts into a support group also helps in effectively managing permissions. Permissions granted to a support group are automatically transmitted to all contacts related to the group. This saves your time in individually assigning Permissions to multiple contacts for the same actions or functions.

Actions like enabling or disabling Service Feedback can also be managed at Support Group Level.

Default Support Groups

Nimsoft Service Desk provides for three Default Groups - Administration, Self-Service, and Public; there is also a System defined group named Not Specified. The purpose of the default groups are:

Self-Service Group: All contacts who are assigned Self-Service License automatically become part of the Self-Service Group (as Primary Group)

Public Group: All other contacts who are assigned Fixed or Floater License become members of Public Group

Administrator Group: The first contact configured as the Application Administrator (defined during slice provisioning) becomes the first member of the Admin Group. Any member who undertakes Administrative tasks can be made part of the Administrator group.

Members of the Self-Service Group by default get access to the Self-Service User Interface of the application upon logging it. Members of Administration by default get access to the full suite of forms and modules of the Application. Hence, those contacts involved configuration and set up of Nimsoft Service Desk can be made member of Administration Group.

For all three groups, the Used For Permissions is checked. While you can modify the Group name and other details, you cannot remove the Used for Permissions Checkbox. You can add the other Used For Options to the default group.

You can add new support groups as per your specific requirements. You can then manage permissions to various modules by enabling or revoking permission for a form or application module to that support group.

You can also set the Next Escalation Group for a Support Group, and define which group takes up action on a ticket if the Support Group to which the ticket was initially assigned fails to act on the ticket within defined SLA target time.

The actions you can take related to Manage Support Groups are explained below.

Create and Modify Support Group

You can manage Support Groups from the Manage Support Groups link under Application Setup. Clicking on this link displays the Manage Support Group and a list of Support Groups that are active in your Nimsoft Service Desk instance.

The screenshot displays the 'Application Setup (Manage Support Groups)' window. On the left, there are three red boxes with labels: 'List Filters', 'Support Group List', and 'Support Group Details'. The 'Support Group List' shows a table with the following data:

Group ID	Group Name	Description
25	OnCall Level3	AutoOpen OnCall Level3
30	OnCall Level1	AutoOpen OnCall Level1
32	Web Services L2	Web Services Support

The 'Support Group Details' section for 'Web Services L2' includes the following fields and options:

- Group Name: Web Services L2
- Description: Web Services Support
- Group ID: 32
- Status: Active
- Email: webservices@support.com
- Phone Details: 0002423377
- Next Escalation Group: Web Services (L3)
- Used For: ☒ Permission, ☒ Notification, ☒ Assignment, ☐ Approval Group, ☒ SLA Escalation
- Members: A table with columns for Name, Location, Business Hours, Primary Group, Group Lead, and Status. The table contains one row for 'Bartone' with 'Self Primary' and 'Agent AP' as locations, 'No' as Primary Group and Group Lead, and 'Active' as Status.

You can also choose to filter the list using the available options. You can click on any Support Group name in the list and the details get populated in the form below.

The Manage Support Group form allows you to modify details related to an existing Support Group. The modification takes effect and all related entities where the support group is used get modified accordingly.

You can manage the Status of the Support Group (active or inactive), relate contacts to the support group, define actions that the support groups can be used for, and enable or disable the group’s ability to participate in Service Feedback Process.

Create New

You can use the form to create new Support Groups by specifying the minimum required information i.e. Group Name, Description, and Used For ; and any other details like Group Type, Subtype, etc. You can specify a new Group Type or Sub-Type or choose from options created earlier. You can also specify the Screen Refresh Interval so that contacts related to the support group don’t have to manually refresh their screen.

If your Support Group has an Email ID and Phone Number, (separate from the Email ID and Phone Number of individual members of the Support Group), you can provide the Email ID and Phone Number for the Support Group in the relevant fields.

This will enable notifications to be delivered to the Support Group Email ID and/or phone number*.

Set Next Escalation Group

You can select any Support Group that you have configured earlier, as the Next Escalation Group of the new Support Group you are configuring. For example, if you are configuring a Support Group as Web Services L2 Support Group; you can select a Web Services L3 Support Group as the Next Escalation Group.

The screenshot shows a web form for configuring a support group. At the top, it says 'Support Group #32 : Web Services L2'. There are three tabs: 'Contact Details', 'Next Escalation Group', and 'Apply Changes'. The 'Contact Details' tab is active. It contains fields for 'Group Name' (Web Services L2), 'Description' (Web Services Support), 'Email' (webservices@support.com), 'Phone Details' (8662423377), 'Type' (dropdown), and 'Sub Type' (dropdown). The 'Next Escalation Group' tab is also visible, showing 'Group ID' (32), 'Status' (Active), 'Refresh Table Every(Mins)' (5), and 'Next Escalation Group' (Web Services (L3)). There are also checkboxes for 'Disable Service Feedbacks' and 'View Organization Tickets'.

This can be used as the escalation rule when configuring Service Targets to implement Service Level Management.

Define Used For

While managing Support Groups, you have to determine what actions the support group can be used for. The available options are ‘Permission, Notifications, Assignment, Approval and SLA Escalation’. You have to choose at least one option and you can choose multiple options, if necessary.

Support Group Detail

Support Group #32 : Web Services L2

Apply Changes

Create New

Delete

Group Name

Web Services L2

Description

Web Services Support

Group ID

32

Status

Active

Email

webservices@support.com

Phone Details

8662423377

Refresh Table Every(Mins)

5

Type

Sub Type

Next Escalation Group

Web Services (L3)

☐ Disable Service Feedbacks

☐ View Organization Tickets

Used For

☒ Permission ☒ Notification ☒ Assignment ☐ Approval Group ☒ SLA Escalation

Support Group Used For

Defining a Used For allows you to control the availability of the groups in related lookups. For example, when a Support Group is configured as Used For Notification; the Support Group will be available for use in To, CC and/or BCC fields of Communication Templates.

Similarly; if a Support Group isn't configured as Used for Permissions, the group name will not be displayed in any Permissions Lookup.

SSU View Organization Tickets

For the Self-Service Group, you can control whether members of this group can 'View Organization Tickets'.

If the View Organization Tickets checkbox is checked, and the related Configuration Parameters SSU_VIEW_MY_REQUESTS_ONLY is set to NO; Self-Service Users will be able to view tickets logged by others in their organization. By default this ability is disabled. You can enable this option if appropriate to your organization.

Note: If Organization Details at all three levels i.e. Organization, Site and Location are defined; the Self-Service Users can view tickets logged by only those contacts who belong to the same Organization, Site and Location; and not other contacts related to the Organization but belonging to other site(s) or location(s).

Relate Contacts

You can relate contacts to the Support Group by using the Add action button. Clicking on this displays the List of Users lookup. You can choose multiple contacts from the list and relate them to the support group.

If a contact is already related to another group which has been set as Primary Group; you will get an option against the contact name to **Set As Primary**. If you click on this option in the table, the selected support group will get set as the contact's Primary Group.

You can also designate any contact as the Group Lead of the Support Group. By default, no contact is set as a Group Lead. To set a Group Lead, you can click on the 'No' in the row containing the Contact record. This will set the selected contact as the Group Lead. This can be used for actions such as SLA escalations, setting contextual approver or reviewer for the ticket etc.

When a user is assigned 'Self-Service License', the user by default becomes member of the Self-Service Group as Primary Group.

Although they can be related to multiple groups, members of this group can access and perform only those actions that are available from the Self-Service User Interface.

Relate Location

You can relate a Support Group to multiple Organizations. This is particularly helpful if you plan to enable the Organization Based Security feature. By relating a Support Group to an Organization, all contacts related to the Organization inherit the relationship to the Organization. This allows related contacts to view and work on tickets and configuration items related to the organization.

You can add Organization using the Add Location action button in the Location tab. You can choose to relate only Organization; or Site and Location as relevant to your business needs.

Note: If you relate a Support Group to a Site, or Site and Location; access to tickets and CIs will be limited to only those records that are related to that Site or Location of the Organization.

Manage Support Group Business Hours

You can define Support Group Business Hours by associating schedules for the Support Group. You can associate multiple Schedules for a Support Group. The Support Group business hours can be used to manage ticket assignments; SLA targets calculations, and other such actions.

You can view all schedules associated with the Support Group from the Business Hours Tab. Clicking on the link displays all schedules associated with the Support Group

You can edit or delete a schedule; or add new schedules using the Add Schedule action button. The actions you can take related to Support Group Business Hours are:

Create Schedule

To create a schedule, you have to specify Schedules Start Date; and if you want the schedule to be valid only for a specific duration, you can specify an end date.

You can change the Time Zone at which the schedule applies; and the days at which the schedule applies and attach a Holiday list to the schedule.

Attach Holidays

Depending on the nature of the Schedules, you can specify a schedule for Holidays (to be applied only on holidays); a schedule to exclude holidays, and specify days when the schedule applies.

It is not mandatory to associate a schedule for a Support Group. If no schedule is associated; the default schedule gets applied as available 24 X 7. Therefore, depending on the nature of work done by the support group, you can choose a schedule or decide to not associate a schedule with the support group.

Manage Support Group Checkpoints

Some points to check back when managing Support Groups are:

- A Support Group can be used for Permissions, Notifications, Assignment, Approval or SLA Escalation only if the relevant check box is checked

- If Support Group Email ID or Phone number is set, notifications will be sent to the support group contact ID. If not, notifications get sent to individual members of the Support Group
- A Support Group can be set as Next Escalation Group for another Support Group, to be used in SLA escalation is to be configured to allow automatic escalation action.
- All Self-Service Users by default become members of Self-Service Group as Primary Group
- Self-Service Group can be given permission to View Organization Tickets by checking the relevant checkbox in the support group records
- Multiple Schedules can be associated with a Support Group
- If no Schedule is associated, the Support Group availability is considered to be 24 X 7.

How Do I

Below are some actions you can take related to managing Support Groups.

Enable Self-Service Users to view My Organization's tickets

For enabling Self-Service Users to view Organization Tickets; the setting has to be enabled in the Self-Service Support Group record and setting the appropriate Slice Configuration.

To enable Self-Service Users to view My Organization's tickets:

Step 1: Click on the Manage Support Groups link under Application Setup.

Step 2: Choose the Self-Service User Group from the list of support groups.

The details of the Self-Service User group will be populated in the Configure Support Groups form.

Step 3: In the Support Group record section, Click on the View Organization Tickets checkbox.

This indicates that Self-Service Users can view tickets logged by others in their Organization. To complete this functionality, you will also have to set the appropriate value in the Manage Config Parameter form.

Step 4: Click on the Manage Config Parameters link under Application Setup. A list of all Slice Configuration Parameters will be listed in the form.

Step 5: Filter the list using Parameter Category. Click on Parameter Category - Self-Service. A list of all Config Parameters related to Self-Service User functionality will be displayed.

Step 6: Click on Parameter Category SSU_VIEW_MY_REQUESTS_ONLY. The details of the parameter and parameter value will be displayed in the form below.

Step 7: Set the Parameter Value to NO.

This will allow Self-Service Users to view tickets logged by others with the same Primary Organization as the logged in user.

Unless the setting is enabled in BOTH Support Group record and Slice Configuration, the functionality will not work.

Note: The Self-Service User can view tickets logged by others users who have the same Primary Organization i.e. same Organization, Site and Location if Site & location is related to the Primary Organization of the Self-Service User.

If you explicitly want a Self-Service User to view all tickets logged by everyone in the Organization (including all Sites and Locations related to the organization) relate the contact to only the Organization (without relating Site and Location) and make this Organization record as Primary Organization.

You can then relate the contact to the same organization; with a relevant site and location; without marking that as the Primary Organization. Thus the contact will be related to multiple organizations (one being the Primary Organization)

Create Support Groups

You can configure Support Groups to group contacts on the basis of their specialization or functional expertise or geographical location, according to their role in the IT Support activities.

To create Support Groups:

Step 1: Click on the Manage Support Groups link under Application Setup. A list of all Support Groups will be displayed in the list.

You can view details of an existing Support Group and modify the record, or create new Support Group in the form below. To create a new Support Group,

Step 2: Click on the Create New action button.

Step 3: Enter the Group Name and Description. Both fields are required fields.

You can choose a Group Type and Sub-Type if needed, though this is not mandatory.

Step 4: Enter the time interval at which you wish the Application screen to refresh for this support group. You can add time in minutes.

This is needed particularly for Service Desk Agents who work real-time with tickets. The screen will be refreshed at regular interval without the user having to manually refresh the screen.

Step 5: Select an appropriate Used For options to determine the actions of the support group. You can choose at least one option. You can select all if appropriate.

This controls the display of the support group in the lookups related to that function, and thereby ability of the Support Group to participate in that function.

Select 'View Organization Tickets' checkbox to enable the support group to view Organization tickets. This field will be enabled only for Self-Service User Group.

Step 6: To control ability of the Support Group to participate in the Service Feedback process, check on the Disable Service Feedback checkbox.

Step 7: Click on Apply Changes to create the new group.

When you save the Support Group record, the Members tab and Business Hours tab get activated on the form.

Step 8: Click the Add action button to view the List of Users lookup.

You can relate contacts to the Support Group from this lookup.

Step 9: Click in the checkboxes to choose multiple contacts and click on Select.

The selected users will get related to the Support Group. You can make this as the Primary Group for any of the related Contacts.

Step 10: Configure a Schedule for the Support Group in the Business Hour Tab. You can configure multiple Schedules for the contact. This helps in Auto-Routing and SLA monitoring related aspects of the ticketing functionality.

Note: If the contact is not related to any other Support Group, this Support Group will default reflect as Primary.

If you don't configure a Schedule, the business hours of the Support Group will be considered by default as 24X7.

Configure a schedule for a Support Group

You can define Support Group Business Hours by associating schedules for the Support Group. You can associate multiple Schedules to manage ticket assignments, SLA targets calculations and other such actions.

To configure a schedule for a Support Group:

Step 1: Click on the Manage Support Groups link under Application Setup. From the list, select the Support Group for which you wish to configure a Schedule.

The business hour tab gets activated on a new Support Group record after the record is saved.

Step 2: Click on the Business Hours tab.

If any schedule is listed with a Support Group, it will be displayed in this tab.

Step 3: Click on the Add Schedule action button to open the Schedule lookup.

Step 4: Enter the Schedule Start Date, Start Time and End Time. All three fields are required fields. Specify the end date if you want the schedule to be valid only for a specific duration.

Step 5: Select a time-zone from the dropdown list. This will be the time-zone for that schedule associated with the Support Group.

Step 6: Select days of the week that the schedule applies to.

Step 7: Relate a Holiday Group if the Schedule is to be excluded on holidays.

Step 8: Click on Apply Changes to create the new Schedule for the Support Group.

If no schedule is associated with a Support Group, the default schedule is taken as 24 X 7.

Frequently Asked Questions

Below are answers to some questions you may have related to managing Support Groups.

How is the primary group different from the other groups that a Contact is associated with?

While contacts can be related to multiple Support Groups, any one support group is identified as Primary. This indicates that the contact belongs mainly to this group.

For all contacts with Self-Service License, the Primary Group by default is Self-Service Group. They can perform only those actions which are available from the Self-Service Interface.

Aspects like participation in Service Feedback is also controlled by Primary Group. If Disable Service Feedback is checked for the Support Group, all contacts with that Support Group as Primary Group will not be able to participate in Service Feedback process.

Can a user view details of which groups he/she is a member of?

Yes, Service Desk Agents can view details of the support groups that they are members of. They can access this information from their own contact record. In the Application Tab of their contact record, they will be able to view information on all Support Groups that they are members of and about the Primary Group.

Also, on the Home Page (where the Service Desk Agents view Ticket List) the Filter Option allows them to filter ticket list by Assigned to Group. This dropdown lists all Support Groups that the Logged in user is member of.

Can members of the same group belong to different Organizations or sites or Locations?

Yes; members of one support group could belong to different organization, site and/or location. For example; you could have a support Group called L1 Network Support and contacts related to the support group could be in different sites like London, New York, Singapore etc. depending on their physical location.

What is the function of the Used For Permission, Notification, Approval, Assignment, and SLA Escalation checkboxes?

Checking the Used for (Permission, Notification, Approval, Assignment, and SLA Escalation) enable the ability for the support group to be available for the above actions. You can choose one or all options available.

If a group is defined as Used for Permissions, then the Group will appear in the Permissions lookup and you can assign permissions to the group (and contacts related to the group). Similarly, unless a group is set as Used for Assignment, the support group name will not be displayed in the lookup for assignment related actions and auto-routes.

Is there a restriction of how many groups a contact can be part of?

No. There is no such restriction on the number of groups a contact can be part of. Depending on the different actions a contact performs, you can relate the contact to multiple groups.

Is there any restriction on how many contacts can be part of a group?

There is no restriction on the number of contacts that can be part of a Group. All contacts who perform a specific action can be part of that group.

Can the same group be used for more than one purpose (say Notification as well as Assignment?)

Yes, a Group can be used for one or more purposes. You can check the used for option for up to all 5 available options of Permissions, Assignment, Notification, Approval, and SLA Escalation.

At least one option has to be checked for the Support Group record to be saved.

Is it mandatory to define business hours for a Group?

No; you don't have to define business hours for a Support Group. If you don't specify business hours for the group, by default the support group availability is considered as 24 X 7.

Defining support group business hours provides information on Support Group Availability, which can in turn be used for calculations like SLA Monitoring, etc. Therefore, if a group is going to be available only for specific time; defining a business hour would help. It is sometimes convenient to configure Support Groups with a schedule in such a way all contacts for whom it is primary group, all have the same work schedule.

What do the fields Group Type and Sub-type signify? Can I create new group type or sub-type, or am I limited by some system defined types and sub-types?

This is an additional way provided to classify group on a basis entirely defined by customer's Application Administrator. You may wish to classify a group based on the type of activities it does, for example, a Support Group - ERP Support Group could have a type as Software Support and a Sub-type as External Vendor. Classifying the groups in this way could help in specifying the actions the group takes.

These are not mandatory fields; so you may choose not to add a group type or subtype. You can add new type or subtype depending on how you wish to classify the group. Once you specify a new group type/subtype, the detail will be available in the lookup and you could choose to use one of the available options instead of create a new one.

If I don't check the Disable Service Feedback flag for the group, will the group automatically receive service feedback forms?

The disable functionality is controlled at three main levels. First is the Contact's Primary Organization Level. If the disable service feedback flag is checked for the organization, contacts related to the organization are excluded from the service feedback process.

Thus, if the Disable Service Feedback flag is checked for Organization, but not for contact's primary support group, contacts will still not be able to participate in the feedback process.

What is the View My Organization Tickets Checkbox on the Support Group form? What function does it serve?

The view organization checkbox is a functionality that is available only for the Self-Service Group. It allows Self-Service Users to view tickets logged by other users who belong to the same Organization, site and location (depending on the levels related).

If you wish to allow Self-Service users to view tickets logged by others in their organization, you can check the View Organization Tickets checkbox. If the View Organization Tickets checkbox is checked and the Slice Parameter SSU_VIEW_MY_REQUESTS_ONLY values is set to NO, Self-Service Users will be able to view tickets logged by others users who belong to the same Organization, Site and Location.

Can a group have multiple schedules? How does this impact the support groups' working?

You can associate multiple schedules with a support group. For example, you could have one schedule to be applied only for holidays or a schedule to exclude holidays. Similarly, you could have one schedules for a specific part of the week; and one for another (like weekdays and weekends).

Applying schedules is used only to measure availability of a support group and does not affect the support group in any other way.

What are the implications of not defining the Business Hours for a Group?

If support group business hours are not defined, then by default the group is considered to be available 24 X 7.

Chapter 13: Manage Roles

Overview

Role refers to the actions and activities required for or required from a person or group. For example, Change Manager, Service Delivery Supervisor, etc. In Nimsoft Service Desk, individual contacts and support groups can be brought together into a Role for managing permissions.

When assigning Permissions, you can assign permissions to a Role and this gets automatically transmitted to all members of the Role.

A Role can also be used for sending communications. You can mark a communication to a Role by selecting the Role in the To, CC, or BCC fields. The communication reaches all members of that Role. Some of the actions you can take to manage Roles are explained below.

Create and Modify Roles

You can manage roles using the Manage Roles link under Application Setup. Clicking on this link displays a list of all available roles that have already been configured.

The screenshot displays the 'Application Setup (Manage Roles)' window. It features a search bar at the top right. Below it is a table listing roles:

ID	Role Name
54	HR Manager / Escalation
55	Level 1 Agent
56	Level 2 Agent
57	Level 3 Agent
58	Service Desk Supervisor
59	Agent Default
60	Change Manager
61	Administrator
62	NO Test Role
63	Customer Support Services

Records 1 to 13 of 13

The 'Roles Details' section shows the details for 'Role #20: Nimsoft Service Delivery Manager'. It includes a 'Role Name' field with the value 'Nimsoft Service Delivery Manager'. Below this are two tabs: 'Granted to Members' and 'Assigned Permissions'. The 'Granted to Members' tab is active, showing a table of members:

	Type	Contact Group Name
☐	User	Domestic, Domestic
☐	User	Domestic, Store

Records 1 to 2 of 2

There are no system defined roles and no filters for narrowing the list as Roles have no further division (like Type). You can search for a Role by entering the Role Name in the Search window. You can click on a Role and the details get populated in the form below.

You can modify details related to the Role, like change Role Name or modify contacts related to the role. The changes get reflected on all other areas where the Role is used (like permission look up etc.).

You cannot make a role Inactive and then make it active again. However, you can delete a role to remove it permanently from the application. When a Role is deleted, all Permissions assigned to the Role (and thereby to related contacts and Support Groups) get removed.

Manage Role Relationships

You can also create a new role using the Manage Roles form. To create a new role, you have to specify Role Name and save the new role.

After you save the Role, the options to associate Contacts or Support Groups to the role gets enabled. You can then add contacts or support groups to the role. You can also remove Contacts or Support Groups added to a role as required.

The Assigned Permissions tab on the Role record displays a list of all actions and permissions assigned to a role. This tab only displays the Permissions available for this role. You cannot add permissions or manage permissions from this tab.

Permissions get assigned to the Role from the Manage Permissions form on the respective record to which you want to assign or revoke permission.

Manage Roles Check Points:

Some points to bear in mind when managing Roles are:

- Multiple contacts and multiple Support Groups can be grouped into a role
- A role cannot be made inactive. Deleting the role removes the record permanently
- Permissions assigned can only be viewed from the Role record; but cannot be managed from within this form.

How Do I

Below are some actions you can take related to reports.

Configure a Role

In Nimsoft Service Desk, individual contacts and support groups can be brought together into a Role for managing permissions. You can assign permissions to a Role, which then gets automatically transmitted to all members related to the Role.

To configure Roles:

Step 1: Click on the Manage Roles link under Application Setup. The list of active roles will be displayed.

You can view and modify details of an existing Role as well as configure a new Role in the form below.

Step 2: Click on the Create New action button to create a new Role.

Step 3: Enter a Role Name, which is a required field.

Step 4: Click on Apply Changes. The new role will be saved.

The Granted to Members tab now gets activated, and the option to associate Contacts or Support Groups to the role now gets enabled. The Permissions Tab also gets displayed on the record.

Step 5: Click on the Add Contact to add Contacts to the Role or the Add Group button to relate Support Groups to the Role.

You can select multiple contacts/support groups from the Lookup and add them to the Role at a time.

You can remove any contact or support group added to the Role by checking on the Contact name and clicking on Remove.

Deleting a Role will result in the Role being removed permanently from the system. Permissions transmitted via the Role to all related Contacts will be disabled when the Role is deleted.

Frequently Asked Questions

Below are answers to some questions you may have related to managing Roles.

How does creating a Role help with managing the service support activities?

A Role is used for managing permission in Nimsoft Service Desk. Contacts and more than one support groups could be undertaking similar kind of activities and could therefore need access to similar permissions in the application. Roles can be used to manage permissions more effectively.

For example, there could be different Approval Groups, which could all be grouped into a Role of Approver. Permissions to access My Outstanding Approvals link in the Navigation Menu can be given to this Role. This will result in consuming less time than the time taken to giving permissions to each group / contact undertaking this activity.

Can there be more than one Role record with the same Role Name?

Yes, the application does not enforce unique values for a Role Name. But it is not advisable to create more than one role with the same name as there could be conflict in recognition of the name by the system.

How do permissions get associated with the contacts/groups associated with a Role?

When permission is enabled for a role, automatically all contacts associated to the role (either directly or by virtue of the support group membership) get the permission.

Is it possible to modify a Role Name for an existing Role record where the Role is associated with a Contact or Support Group?

You can modify a role name, if required. When the Role name is modified, the changed name will be displayed in the Permissions Editor in all places where Permissions can be assigned to the role. Similarly, in the Name Search Lookup for relating a Role to Communication Templates, the modified Role name will get displayed automatically.

What happens when user tries to delete a Role record? How does deleting a Role impact the associated Contacts or Support Groups?

A Role can be deleted. Deleting the role leads to the record being completely removed from the system.

However, when a role is deleted, the relationships to Contacts and Groups related to the deleted role will also get lost. Therefore, permissions transmitted to the Contacts and Support Group via that Role will no longer be available to the related Contacts and Support Groups.

What happens when a Contact is associated with a Role and the Contact record is made Inactive?

If a contact associated with a role is made inactive, it does not in any way impact the Role or the other contacts associated with the role. The contact will continue to be listed in the contact list of the Role record. The relationship of contact with the Role is not deleted.

Can Role be used for the Assignment of tickets as is done for Support Groups?

Roles cannot be used for assignments. They are available only of managing Permissions and for identifying recipients for a Communication Template (whereby the notification can be sent to all members of the Role).

Where do role based permissions become applicable?

Role based permission is applicable to all functions where permissions is applied. This includes Navigation Menu, Toolbar Options, Knowledge Articles, Workflow Actions, Ticket Templates, and Communication Templates.

Is a Role associated with an organization, site or location; and does it get impacted when there is a change to the Organization, Site or Location details?

Role is not directly associated to an Organization, Site or Location. Contacts from any organization, site or location can be assigned to one role. Making an organization inactive does not impact the role. It continues to remain the way it is. However, some of the contacts or support groups associated with the role could become inactive when their primary Organization, Site or Location is made Inactive.

Chapter 14: Manage Holidays

Overview

As every Organization observes some holidays from the routine work; it is expected that services will not be available as per routine on holidays.

In order to plan and publish holidays, and specify workarounds for support related activities on holidays, Nimsoft Service Desk allows you to create multiple holiday groups and associate holidays with Support Group business hours, auto-routes, scheduled activities, etc.

Create and Modify Holiday Groups

You can manage holidays from the Manage Holidays link under Application Setup. Clicking on this link displays a list of Holiday Groups that have been configured. There are no filters as Holiday Groups do not have any further classification.

There are no system defined Holiday Groups. You can search for a specific Holiday Group by entering the Holiday Group name in the search window.

The screenshot displays the 'Application Setup (Manage Holidays)' window. It features a search bar at the top right. Below the search bar is a table titled 'Holiday List' with the following data:

ID	Holiday Group Name	Description
6	USA 2010	USA Holidays 2010
7	UK London 2010	UK London 2010 Holidays
8	Singapore 2010	Singapore 2010 Holidays
9	Banaru India 2010	Banaru India 2010 Holidays

Below the table, it indicates 'Records: 1 to 4 of 4'. The 'Holiday Details' section for 'Singapore 2010' is shown below. It includes a 'Holiday Group Name' field with 'Singapore 2010' and a 'Description' field with 'Singapore 2010 Holidays'. Below these fields is a table of individual holidays:

Holiday Date	Holiday Description	Renew Yearly?
31/01/2010	New Year's Day	Yes
14/02/2010	Chinese New Year - 1	No
15/02/2010	Chinese New Year - 2	Yes
22/06/2010	Good Friday	No
29/09/2010	Labor Day	Yes

At the bottom of the details section, it shows 'Records: 1 to 5 of 5'. There are 'Create New' and 'Delete' buttons. At the very bottom, there is a 'Holiday Title' field with '2010-2011' and a 'Renew Yearly' checkbox which is checked.

When you click on a Holiday Group name from the list; the details get populated in the form below. You can view details of holidays in that group and modify the details as required. You can add or delete individual holidays from a Holiday Group. The Holiday record gets completely removed from the Holiday Group (it cannot be made active or inactive).

To configure a new Holiday Group; you can add Holiday Group Name; and add Holidays dates to the group. If a Holiday being added to the Group falls on a different calendar day each year; or if the inclusion of the Holiday needs to be reviewed; you can check on Renew Yearly. In such a case, the holiday will not get carried over into the next calendar year automatically.

You can delete a newly configured Holiday Group from the list; and the Holiday Group record gets permanently removed. However, if a Holiday Group is associated with other records such as an Auto-Route or schedule; it cannot be deleted. You will get an error message notifying that the Holiday Group cannot be deleted.

You can relate Holidays Groups to various schedules like Support Group Business Hours, CI Service Hours, Auto-Routes etc.

Manage Holidays Check points

Some points to bear in mind related to managing Holidays are:

- A holiday group can contain fixed holidays and dates that need to be reviewed yearly
- For Holidays that fall on different dates, remember to check Renew Yearly checkbox.
- Holiday Groups that are already related with other active records like Auto-Routes or Schedules, the record cannot be deleted.

How Do I

Below are some actions you can take related to managing Holidays.

Create or Modify a Holiday Group

Nimsoft Service Desk allows you to plan, create and publish Holiday Groups that can be associated with different schedules like auto-routes, support group business hours, scheduled activities, etc.

To create or manage a Holiday Group:

Step 1: Click on the Manage Holidays link under Application Setup to displays a list of Holiday Groups that have been configured.

Click on a Holiday Group name from the list to view the details. You can modify existing Holiday Group or create a new Holiday Group in the form below.

Step 2: Click on Create New button to create a new Holiday record.

Step 3: Enter the Holiday Group name, which is a Required Field. You may add a description if required. However, this is not mandatory.

Step 4: In the Holiday Date field, click on the calendar icon to choose a Holiday Date. It is mandatory to choose at least one Holiday Date to save the Holiday Group record.

You can add a description to the Holiday Date to indicate what the Holiday is for. You can choose as many Holiday Dates are required for the Holiday Group.

Step 5: If the holiday is to be renewed yearly (where the holiday falls on a different calendar date each year), check on the Renew Yearly checkbox.

Step 6: Click on Apply Changes to save the details.

The new Holiday Group will be configured.

You can modify a Holiday Date to add more holidays or remove a holiday from the Group. Deleting the Holiday Group will result in the Group being removed permanently from the system.

You cannot delete a Holiday Group that is associated with other records such as an auto-route or schedule. You will get an error message notifying that the Holiday Group cannot be deleted.

Frequently Asked Questions

Below are answers to some questions you may have related to managing Holidays.

What are the different entities with which I can associate a Holiday Schedule?

A holiday schedule can be related to Auto-routes, support group business hours, service hours for CIs, and scheduled activities. It also plays role indirectly in SLA monitoring through the Availability schedules of Groups and Service availability schedules for CIs/ Services.

What does the field “Renew Yearly” indicate? When should it be flagged as Yes?

The Renew Yearly field indicates that the holiday should be reviewed when creating Holiday list for next year. Some annual Holidays (of other cultures) do not always fall on the same date of Christian calendar. The holiday date for such holidays will need to be reset in the next calendar year.

This field should be checked for holidays where the date changes every year (for example, Indian Festivals) as a reminder to user creating the calendar for coming year.

Can I modify a Holiday Group Name after it is already associated with other records or transactions?

Yes, you can modify the Holiday Group name and add or remove holidays from a Holiday Group that is already associated with other records. The New modified Name will be displayed where ever the Holiday List name is to be displayed. The Name change does not change anything else.

What happens when user deletes a Holiday Group where the Holiday group is associated with Support Groups and Auto Route?

A Holiday Group cannot be deleted after it is associated with other records such as Auto-Routes, Schedules, etc. When the administrator tries to delete the Holiday Group, a message is displayed indicating that the Holiday Group cannot be deleted.

How does deleting a Holiday listed in the Holiday Group affect the working of the entities with which the Holiday Group is associated?

Individual holiday listed in a Holiday Group can be deleted as required. If an individual holiday is deleted, application will consider it a working day. If a new Holiday is added, application shall consider it as a Holiday while applying the Holiday List to the entities.

Can I create more than one Holiday Group with the same name?

No. A Holiday Group Name must be unique. The Application displays a message if administrator tries to create a Holiday Group with the same names as an existing group.

Chapter 15 - Manage Categorization

Overview

In Nimsoft Service Desk, categorization is applied to Tickets and Configuration Items.

A four level categorization of Class, Category, Type and Item can be defined in a central pool, and be made available for different forms as relevant. This categorization can be then used for Tickets or Configuration Items as appropriate.

Create Categorization Records

You can manage categorization from the Manage Categorization link under Application Setup.

Clicking on this link displays a list of all available categorization. You can filter the list using available filters or search for a specific categorization by entering appropriate search text in the search window.

The screenshot displays the 'Application Setup (Manage Categorizations)' window. It features a table of categorization records and a detailed view for a selected record.

List Filters: Filter By, Form Name, Status, Search

Categorization List:

ID	Form Type	Categorization Class	Categorization Category	Categorization Type	Categorization Item
92	Change Request, Inci...	ERP	All Modules Common Issues	Menus	
115	Change Request, Inci...	VMware	Work Station		
284	Service Request	HR			
89	Change Request, Inci...	Servers	File Server	HP	NFS
295	Change Request	Approvals	Requester	Manager	
72	Service Request, Cha...	Operating Systems	Linux		
218	Configuration Item	Networking	Switches	Cisco	Catalyst 48 ports
112	Change Request, Inci...	ERP	SCM Module		
292	Change Request, Inci...	Engineering SW			
304	Change Request, Inci...	Security	Scheduled Activity / Tasks		

Record(s) 1 to 20 of 130

Categorization #221 - Power

Related To Forms: Configuration Item, Service Request, Problem, Incident, Change Requi... Status: ☒ Active ☐ Inactive

Categorize

Class: Power Category: UPS Type: APC Item: 3 KVA

Image Name: No Image

Image Description:

To view details of a categorization listed in the table, click on the item listed. The details will get populated in the form below.

You can modify an existing categorization by changing details like related to form(s); changing class name, or adding or deleting details like category, type or item. When saved, the changes get applied to all records where the Categorization has been used; including closed tickets.

You can manage the Status of a Categorization record (active or inactive)

Create New

You can create new Categorization using this form. To create new categorization; you have to specify the forms to which the categorization can be applied. The look up lists the forms to which the categorization can be related; which includes Service, Incident , Problem , Change, Task or Configuration Item. You can choose multiple forms to which the categorization gets related.

Specify CCTI

To create a Categorization, the other mandatory field is Class. You have to specify at least a Class for a Categorization. You can further define category, type and item; though these fields are not mandatory. There can be several categories related to a class; and several types related to a category and several items related to a type. Organizations must generally choose categorization carefully with a long term perspective.

You can also associate an image with a categorization and provide a description if required.

Manage Categorization Check points

Some points to consider while creating or modifying Categorization records are:

- A Categorization record can be related to multiple forms (ticket forms or Configuration Item form). The CCTI becomes available to the form which it is related to.
- Categorization can be used as a matching condition for Auto-Routes, Action Options etc.
- Modifying a Categorization record after it has been associated with other records (like auto-routes) can cause the related workflow to fail; and hence due planning and caution is advised before modifying CCTI records.

How Do I

Below are some actions you can take related to Categorization.

Manage categorization records

In Nimsoft Service Desk, a four level categorization of Class, Category, Type and Item (CCTI) categorization is applied to Tickets and Configuration Items.

To create categorization records:

Step 1: Click on the Manage Categorization link under Application Setup to displays a list of all available categorization.

You can view details of an existing Categorization Record in the list, modify an existing record or create new Categorization record in the form below.

Step 2: Click on Create New button to create a new categorization item.

Step 3: Fill in the minimum required information such as Related to Forms.

This will specify the forms to which the categorization can be applied. You can choose multiple forms to which the categorization gets related.

Step 4: Specify the Class of the new categorization item. It is a required field.

You can further define category, type, and item; though these fields are not mandatory.

Step 5: Fill in the Image name if you want to associate an image with a categorization and provide a description if required.

Step 6: Click on Apply Changes to save the categorization item record.

A new Categorization record will be created.

Frequently Asked Questions

Below are answers to some questions you may have related to Categorization

Can tickets and CIs have the same CCTI? Can one CCTI be associated with multiple forms?

Yes; tickets and Configuration Items (CIs) can have the same categorization. When configuring categorization, you can relate it to multiple forms including different ticket forms and CI forms.

Is it possible to use only three or fewer levels for categorization for a particular ticket or CI rather than using all four levels?

Yes; you can skip one or more level of categorization. You can choose to define only Class, only Class and Category, or only Class, Category and Type for a ticket or CI in Manage Categorization, and not define all levels.

However, please note that defining Class is required, while the remaining levels are optional. You can skip them the other three levels after Class is configured.

Is it possible to use only Class, Type and Item (and skip Category) in creating a categorization?

No, to define Type and Item, you have to define Category. This is because each level is incrementally related to the other. For a given class, there are certain categories; for a given class and category, there are specific types; and for a given class, category; and type, there could be items.

As the relationship is hierarchical in nature; you have to specify a higher level entity before specifying an entity lower in the hierarchy.

What is the effect on older records with a CCTI, when the CCTI is modified?

When an existing CCTI is modified, the old records (Tickets and CIs) to which it has been already applied are not updated. They continue with the CCTI as it was before modification. But new records can be linked only to the modified CCTI.

However, changing the CCTI after it is used as matching conditions for Action Options, Auto-Routes, SLA targets, etc., can lead to the entities not getting applied or progress of the ticket failing because a matching condition was changed.

What happens when a CCTI for a ticket or CI is made inactive?

The Ticket or CI record where CCTI was applied remains categorized as per the CCTI which is made Inactive. In its Inactive status the CCTI cannot be applied to new Ticket or CI records.

When an inactive CCTI is made active again, does it affect the CIs that have that CCTI?

When an Inactive CCTI is made active again, it becomes available for applying to new CI records or changing CCTI of existing CI Records. It does not impact CI records where it is already applied.

What happens to open ticket records when a ticket CCTI is made inactive?

Nothing changes for the Ticket. The Inactive CCTI is no longer available for applying to new tickets or changing the CCTI of existing tickets.

The Ticket Template continues to bear the Inactive CCTI. When a ticket is created from such a template, the Ticket also bears the Inactive CCTI.

Chapter 16 – Bulk Process Data

Overview

Processing means to move data from a local system / computer / Application to a server or application where it is stored for use by the application and others to access or later retrieval.

Nimsoft Service Desk enables you to use Bulk Process to import, update and delete large amounts of data related to Organization, Sites, Location, Support Groups, Contacts, Roles , Categorization and Configuration Items. All relevant data can be bulk processed during the provisioning phase.

Bulk processing of data allows creating new data, updating existing records in a bulk mode, and deleting the existing records. It partially validates the data imported and reports errors if the data could not be unprocessed. You can preview the actual Import data before processing.

The relationship between these entities, in terms of relationship of a contact with an Organization, Support Group or Role and relationship of a Configuration Item with categorization record (CCTI) and contact (as owner, user, etc.) can also be captured during Bulk processing.

Manage Bulk Process

You can manage the process of Bulk Import or delete of data from the Manage Bulk Process form.

Application Setup (Bulk Upload Data)

File Name	Name	Description	Process Status	Processed By	Processed Date
Test Bulk Upload.xls	Test Data Import		Waiting	Admin, InteQ	24/02/2011 12:23:52

Record(s) 1 to 1 of 1

Enrollment Data: Test Data Import [Delete]

Step 1: Process File | Step 2: Map Worksheets | Step 3: Map Columns | Step 4: Preview Data | Step 5: Execute Operation | Step 6: Log

Filename: [Browse...] [Upload] [Clear]

Name: [Test Data Import]

Description: [test rtes tes test]

Operation: ☒ Import/Update ☐ Delete

The table above shows a list of bulk process templates that are currently being processed by the application. The table also displays the status of the upload process, and date when the process was initiated.

The steps involved in the bulk upload process are explained below.

Steps to Bulk Process Data

To Bulk Process the data, you need to prepare the Enrollment Data in an Excel sheet (no other spreadsheet formats are currently supported). Having prepared the required information in the defined format, you can initiate the Bulk Process.

Bulk Process is a five step process.

Process File

As the first step, you can specify the location of the document that has to be uploaded. You can specify the file path to where the document is located on your local system.

Once the initial file is identified, it can be uploaded and gets parked in a temporary place.

Map Worksheet

Once parked, in the second step, worksheets in the file are mapped with the appropriate data files in the application. As the naming conventions used by you may differ from the database column names; mapping the worksheets ensures that the appropriate data is moved into the right database.

For example; what is referred to as Organization in the database; may be called Company in your file. Mapping the worksheets eliminates potential data mismatches.

Map Columns

As each record has multiple fields; there is a wide range of data related to each form that will be getting imported. In the third step; columns of each spreadsheet are then mapped to corresponding columns in the database. This helps ensure that the right field value is being processed in the right field.

Preview Data

Having mapped the columns, the fourth step is of previewing the data to check whether all records are appropriate; and further ensure that no changes are needed before the data is uploaded. You can preview the data per worksheet and then initiate the process of upload.

Execute Operation

Once the data import process is initiated, you can view the Import Sheet; which displays a list of imported sheets mapped in a tabular manner. You can view the Status of the import process. Once the sheet has been imported, you can view data on erroneous record, which did not get imported and drill down into the detail of the record to view the error.

Log

As a final step you can view the Logs. This log gives further information on Errors which can occurred during the import process. You can correct the incorrect entries; and initiate the process of bulk process afresh, if required.

To assist with Bulk Process of data; the enrollment sheet is provided to you during the provisioning phase. This helps in capturing all required information in an appropriate format and thus saves on effort to bulk import data.

Bulk Process Operations

The operations that are supported in Bulk Process are explained below.

Delete: The Delete action button indicates Deletion of Session Information.

This allows you the ability to Select a row from the list of Bulk process sessions and delete it. Only the session information and its maintenance form get deleted. The actual data that were processed, added / updated / deleted from database do not get affected.

Operation: Import/Update Delete

The two radio buttons are provided for Operation on Step 1, Process File tab. You have ability to select “Import/ Update” to enable the records to be created into a new record or to update an existing Record in database.

You have the option to select the “Delete” to delete records listed in worksheet data from the database.

Based on the selection in Step 1, in Step 5, Execute Operation tab, the action link in first column becomes “Import” for “Import / Update” operation or “Delete” for delete operation.

The administrator can select “Delete” in Operation to delete records listed in worksheet data. The delete action can remove all worksheet from a File or several worksheets. A record is deleted only if a unique record is identified.

If more than one record are found in the database that meet the Record details, the worksheet record shall not be processed and will appear in the list of Unprocessed records in Log Tab. If a record to be deleted has dependent entities or relationships with other entities, it shall not be deleted.

How Do I

Below are some actions you can take related to Bulk actions.

Prepare list of Organization, Contacts and Support Groups for bulk deletion

You can get a list of existing Organization records or Site records or Location records as an input for delete action using Bulk Processing.

To generate a list of records to be deleted using Bulk Upload Process:

Step 1: Click on Predefined Search under Administration Utilities. Select the Search tab.

Three Systems defined searches for Administrative records get displayed in the table along with their description:

- Organization: A list of all Organizations configured in the system.
- Sites: A list of all Sites configured for Organizations in the system.
- Location: A list of all locations for sites and organizations configured in the system.

Step 2: Select the Defined search you need by clicking on the row.

The Search result tab shall display the details

Step 3: Export the Search result as “CSV” file by selecting the Icon right bottom Corner of the document

Step 4: Retain the records you wish to delete in the exported file.

Step 5: Use the CVS file for deleting the records using delete option available in Bulk Processing of Data.

The data that has been generated can now be used for deleting the records using the Bulk Process.

Frequently Asked Questions

Below are answers to some questions related to managing Bulk Process.

What type of data can I bulk process?

You can bulk upload data related to:

- Organization
- Site
- Location
- Contact
- Support Group
- Role
- Configuration Items

You can specify the nature of relationships between Organization, Site, Location, Contact, Support Group and Role when bulk processing the data. You can also create the CI - Contact relationship and upload this information during bulk process.

Can I bulk process data myself?

Yes, if required, you can bulk process the data yourself. Support will provide you with the Data Enrollment Sheet, which provides the format in which the data to be bulk processed has to be prepared.

Once the data is collected in the required format, you can initiate and complete the bulk process yourself.

It is also advisable to view the document detailing the Bulk Process carefully and to follow the validation steps indicated in the document. If the data upload is not validated, erroneous data will get processed, which could cause delays and disturbances in how the record is used in the application.

Is there a limit on the amount of data that I can bulk process?

No, there is no limit on the amount of data that you can process. You can attempt to upload all required data in one go.

How do I know that the data has been fully processed?

You can view progress of the bulk import and the Import Sheet during the progress of the Bulk Process. The sheet displays the status of the bulk process and also displays an error log, which lists data that could not be uploaded.

What happens if there is an error in the data during the upload process after the bulk process has been initiated?

If there is an error in the bulk process and data mismatch issues are picked, the incorrect records do not get uploaded. The list of incorrect records can be seen in the log tab.

You can view the error message, correct the erroneous data, and initiate another round of bulk process to upload the missing data.

Chapter 17 – Manage Attributes

Overview

Attributes are additional fields that can be used on Ticket and Configuration Items forms for custom defined values for these records.

You can create Attributes that can be commonly used for all ticket forms and Configuration Item records. The same attribute can be used on more than one form, wherever such a field value is needed.

Create and Modify Attributes

The Manage Attributes link under Application Set up allows you to create a pool of Attributes that can be used to create Custom Fields for Ticket and configuration items. The Attributes List table lists all available attributes.

You can view an existing attribute, and modify its values as appropriate. You can also create new Attributes.

To create a new attribute, you have to specify Attribute Name (this is a Required field), Attribute Type, Attribute Unit, Sort Order, and possible Values.

Application Setup (Manage Attributes)

Filter By: Attribute Type Attribute Unit Search

ID	Attribute Name	Attribute Type	Attribute Unit
277	SSU Request Desktop / Laptop OS and Browser	Section Header	
278	HR Telecom set up and Change Request	Section Header	
279	Major Change Cost Estimates	Section Header	
280	Change Approvals	Section Header	
281	Work Group	Section Header	
282	Employee Details	Section Header	
284	Employee Date of Birth	DateTime	
285	Working Hours	Radio Buttons	
286	Application Name	List	

Record(s) 61 to 80 of 84

Attribute # 285: Working Hours Modify Create New Delete

Attribute Name: Working Hours

Unit: Sort Order: Attribute Type: Radio Buttons

Possible Values: 24x7--24x7@x5--9x5

If an attribute is already used with a custom template, you will not be able to delete it. You can modify the details if necessary. For example; you may choose to change Value or Value Type.

However, it is not advisable to modify an Attribute after it has been associated with another action or transaction record, like Workflow Action or Auto-Route, because this could result in loss of backward compatibility.

You can also create attributes called `Section Headers`. These can be used for grouping Ticket Custom fields into relevant sections.

Note: In Nimsoft Service Desk, combinations of Double Tilds (~) and Double Pipes (||) is used with specific purposes. Therefore, these combinations must not be used in any input fields in the application. This can cause the system behavior errors that can be corrected only with engineering intervention.

Manage Attributes Check points

Some points to consider when configuring or modifying Attributes are:

- An Attribute can be used on multiple forms where there is provision for adding fields to the form (All ticket forms and Configuration Item records).
- Attributes can be used as matching conditions for Auto-Routes and Workflow Actions
- Once an Attribute has been used on a form, it cannot be deleted.
- While modifying attributes, due caution must be exercised to ensure the modification is reflected back on all related records.
- Certain special characters must not be used when defining Attribute values. Please refer to the note above for details of these special characters.

How Do I

Below are some actions you can take related to Managing Attributes.

Create Attributes for use on Templates

You can configure a common pool of Attributes that can be used in CI Attributes Templates for Configuration Item records and Custom Fields Templates for Tickets.

To create new Attributes:

Step 1: Click on Manage Attributes link under Application Setup. A list of all available attributes will be displayed in the table.

You can view and modify details of an existing Attribute or create a new Attribute in the form below.

To create a New Attribute:

Step 2: Enter an Attribute Name, which will become the field name that will be displayed when the Attribute is used on a template.

Step 3: In the Unit field below, you can enter a Unit value. However, this is not a required field; hence you may leave it blank.

Step 4: In the Sort Order field, choose a Sort Order for the Attribute. By default, the Sort Order is 0; you may choose not to modify this.

The Sort Order controls the appearance of the Attribute in the list. If not Sort Order is assigned, the Attributes will be displayed in an Alphabetical order.

Step 5: Choose the Attribute Type from the dropdown list. You can set the type of value that the Attribute will accept in this field.

You can choose an Attribute Type as Text, Number, Date time, List, Checkboxes, Radio Buttons or Multi-line text for normal attributes.

Step 6: When you choose Attribute Type as List, Checkboxes, or Radio buttons, the Possible Values field will get enabled. You can enter possible value options for the Attribute in this field.

The Value Options will get displayed in the corresponding Attribute Value field on the form where the Attribute is used.

Step 7: Click on Apply Changes to save the Attribute.

The new Attribute record will be created and will now be available for use on Custom Fields for tickets and CI Attributes Templates.

Attributes can also be configured to be used as Section Headers to group Custom Fields on Tickets.

To configure an Attribute to be used as Section Header on Custom Fields:

Step 1: Follow the above steps 1 to 4 to create a new Attribute.

Step 2: In the Attribute Type field, select 'Section Header' from the dropdown list.

Step 3: Click on Apply Change to save the Attribute.

This Attribute will now be available for using as Section Header to group Custom Fields on a ticket.

Note: If you delete an Attribute from the pool, it will be permanently removed from the system.

Once an Attribute gets applied on a CI Attribute Template or Custom Fields Template, the Attribute cannot be deleted. The application will display a message indicating that the attribute cannot be deleted.

Grouping of Custom Fields using Section Headers is controlled by Slice Configuration Parameter `ENABLE_GROUPING_OF_CUSTOM_FIELDS_INTO_SECTIONS`.

Frequently Asked Questions

Below are answers to some questions related to Attributes.

Where do the attributes created in the Manage Attribute get applied?

Manage Attributes provide the ability to create a reusable pool of attributes that can be used on different forms, like Custom Fields templates for tickets and CI Attribute template for Configuration Items.

An Attribute that is configured can be used on multiple CI Attributes templates and Custom Fields templates thereby reducing the need to recreate the same attribute for different forms.

What type of Attribute Values can I create?

The Attribute values that you can create are Text, Number, Date/time, List, Multiline text, Radio Buttons, Check Boxes, and Section Headers.

What is the Attribute Type- section header mean? When should I use this option?

The attribute type- section header is used for grouping custom fields on tickets into sections. You can configure Section Headers to be used for grouping attributes on a ticket.

When creating custom fields for tickets, you can use a Section Header as a way of grouping related fields. You can then add multiple attributes (custom fields) under the section header.

What happens when I delete an attribute that is used in a ticket form or CI form?

When you delete an attribute, the attribute is permanently removed from the system.

However, please note that the application does not permit deleting an attribute used in Attribute templates. When you try to delete the attribute, you will get a message indicating that the attribute cannot be deleted because it is being used in another form.

What happens when an inactive attribute is made active again?

An attribute from a Pool can only be deleted permanently. There is no Active/Inactive status applied to it.

Chapter 18: Configuration Management

Overview

Organizations have a wide range of Configuration Items like Physical devices, Software Applications, Product or Process Documentation, etc. You can maintain a repository of all Configuration Items within the Configuration Management Module of Nimsoft Service Desk.

Administrators and Service Desk Agents (when given permission) can access the List Configuration Items link and view available configuration items. They can also view details of the CI record, relate the CI to ticket they are working on. They can also search for a specific CI and if permitted, access reports related to CIs.

Besides information related to the Attributes of the CI, the Configuration Item record contains information on Related CIs, Related Tickets, Related Contacts, Service Hours and Attachments. The History tab on the CI record provides information on all changes made to the CI record and the Dependent Data tab lists details of records like tickets, knowledge articles, SLAs etc. that are related to that CI.

The screenshot displays the 'Configuration Management' interface with a 'List Configuration Items' section. It features search filters for Class, Category, Type, Item, and Status, each with a 'Clear' button. Below the filters is a table of configuration items. Red boxes on the left highlight the 'CI Search using CCTI' and 'Configuration Items List' sections.

Name	Function	Identifier	Status	Class	Category
Tomcat Server	Application Server	APS1001TC	Active	Servers	
Laser Printer HP 1300 GR 667	Office Printer	TW-STG-PRT-122	In Use	Printer	Laser
Explorer	Browser		Stolen	Computers	Laptop
Desk Top HP US 649	Personal Computer	TW-ALB-DTP-119	Deprovisioned	Desk Top Hardware	System Box
Laptop HP US 627	Mobile Comp	TW-CHI-LTP-108	In Use	Computers	Laptop
Laser Printer HP 1300 SP 668	Office Printer	TW-SNP-PRT-123	In Use	Printer	Laser
Laptop HP US 632	Mobile Comp	TW-LSA-LTP-113	In Use	Computers	Laptop
Laser Printer HP 1300 UK 665	Office Printer	TW-LON-PRT-120	In Use	Printer	Laser

Record(s) 1 to 16 of 186

Nimsoft Service Desk allows a four level Categorization for Configuration Items; as Class, Category, Type, and Item. The Configuration Item record form provides a range of standard attributes like Make, Model, Warranty Details, Version, etc. that are applicable across most configuration items.

If you need specific attributes to be included, you can create a CI Attribute Template and add new attributes to the Configuration Items by applying the template.

As part of the preliminary configurations, you will create Configuration Item Records into the application after undertaking the pre-requisite activities like defining Categorization (CCTI) for CI Records, building CI records with required attribute Values added to the available attribute fields, identifying and adding additional attributes via the CI Attribute Template, and uploading the CI records into the application.

Configuration Item records can also be Bulk Processed into Nimsoft Service Desk once the necessary details are gathered in the required format.

CI Attribute Templates

The CI record form provides a range of standard Attributes that can be used for most Configuration Items. You can add new attributes by creating new CI Attribute templates and making specific Attributes available to CI records. Configuring a CI Attribute Template is a two step Process. You need to first create Attributes in the common attributes pool under Manage Attributes. You can then choose attributes from this pool to create CI Attributes template. Both these steps are explained below.

Manage CI Attributes Template

The Manage CI Attributes Template link under Application Set up allows you to create new CI Attribute Templates. The CI Attributes Templates form lists all available templates. You can view an existing template in the form area below, and modify details as appropriate.

Application Setup (Manage CI Attribute Templates)

Filter by: [] Status: [] Template Type: [] Search: []

ID	Template Name	Description	Status	Modified Date
-1	Default Attributes	Contains a list of default attributes that are com...	Active	02/03/2011 11:31:21 AM
7	Firewall	Firewall specifications	Active	08/09/2008 01:24:01 PM
11	Switches	Switches Specifications	Active	05/09/2008 05:00:47 PM
12	Servers Class	Servers Class Specifications	Active	08/09/2008 02:30:33 PM
13	Server Category	Server Category Specifications	Inactive	02/03/2009 02:20:19 PM
14	Desk Tops HW Class	Desk Tops Specifications	Active	08/09/2008 02:30:56 PM
15	Laptop Hardware Controller	Laptop Hardware Controller specifications	Inactive	10/01/2009 05:49:51 PM

Records: 1 to 15 of 15

CI Attribute Template #12: Servers Class [Edit] [Create New] [Delete]

Template Name: Servers Class Created On: 08/09/2008 02:30:33 PM Created By: Admin, InteO

Description: Servers Class Specifications Status: Active Modified On: 08/09/2008 02:30:33 PM Modified By: Admin, InteO

Attributes [Related CCTI]

Attribute Name	Attribute Default Value	Unit	Sort Order	Add During Creation?	Unique?	Status
Processor	Intel P 4 S40 (3.260001 M)		1	Yes	No	Active
Processor Speed	3.2	Mhz	2	Yes	No	Active
Memory	4 x 1	GB	3	Yes	No	Active
Hard Disk	80	GB	4	Yes	No	Active
CD	52 X		5	No	No	Active

Records: 1 to 5 of 7

Attribute Details [Create New] [Delete]

Attribute Name: [] Attribute Default Value: [] Unit: [] Attribute Type: [] Possible Value: [] Status: []

☐ Add During Creation? ☐ Update existing Configuration Items? ☐ Enforce Unique Value? Sort Order: []

You can also create new CI Attribute Templates from the CI Attribute Templates form. You can create a new template by specifying a Template Name and saving the record. Once the template is created, you can choose Attributes to be added to the template. The Attributes created in the Attributes pool (Manage Attributes) will be available in the Dropdown List.

You can add multiple attributes to a CI Attribute Template. The value type, unit, and default value get automatically updated on the CI Attribute Template. The Attribute type, text or multi-line text, support upto four thousand characters.

The CI Attribute template can be related to an available categorization (CCTI), and the attributes on the template will be available on all Configuration Item records with matching CCTI.

A CI Attribute Template can be related to more than one Categorization (CCTI) records. It will be available on all CIs with related CCTI. However, if a CI Attribute Template is not related to a CCTI, it will not be available for any CI record.

Managing CI Records

To set up CI records into Nimsoft Service Desk, you need to gather details of all Configuration Items that are part of the IT Service and that are supported by the IT Service/Support Desk. Each item will become a CI record into the application. You can create new CI records, modify existing CI records, or manage the Status of a CI record as appropriate.

Details on how to Manage CI records are given below.

Create CI Record

You can create new CI records from the Create Configuration Item link under Configuration Management. Clicking on this link displays a blank Configuration Item Form.

This form captures basic information about the Configuration Item. Fields like CI Name, CI Class, and CI Organization are mandatory fields. You have to specify appropriate value into these fields before saving the CI Records. CI Organization by default is populated as the Logged in user's Primary Organization.

You can change it to another Organization / Site / Location, if necessary. The other details field like Function, Identifier, Site, Location, Owner, Owner Organization, etc. are optional fields. You can choose to leave these fields as blank fields.

You can also choose to add a Function from the Function Lookup or create a new function for the CI and add an Identifier if you have a unique naming convention for your CI records.

The screenshot shows a web-based form for managing Configuration Items (CIs). The form is titled 'Configuration Item' and has a 'Modify Status' button at the top right. The form is divided into three main sections: 'Configuration Item', 'CI Specifications', and 'CI Attributes'. The 'Configuration Item' section includes fields for Name, Function, Identifier, Status, and Image. The 'CI Specifications' section includes fields for Organization, Site, Location, Owner, and Phone. The 'CI Attributes' section includes a table with columns for Template Name, Attribute Name, Attribute Value, and Unit. The table contains several rows of data, including 'Default Attributes' and 'Attribute Values'. The form also includes a 'Search' button and a 'View All' button.

Depending on the current Status of the Configuration Item in the IT Services and Support, you can choose an appropriate Status for the CI record. If you do not specify a Status, the default status is set as Active.

CI ID details get auto-populated when the CI record is saved. If an image has been associated with a CCTI that is applied to the CI record, the image gets attached to the CI record.

Also, if Attributes and attribute Values have been defined for a Class, these attribute values get applied to the CI record; and the attribute value details are automatically updated.

Once the CI record is created, additional tabs of Related CIs, Related Tickets, Related Contacts, Attachments, Service Hours, and History now appear on the CI Record. You can modify the record to add required relationships and schedule for the CI.

The Dependent Data tab includes information on the dependent entities, their description, the action on termination, and the "Number of records" for each. This information is important when the CI has to be unrelated or unlinked manually before its associated organization is terminated.

All modifications get reflected in the History Tab.

CI Relationships

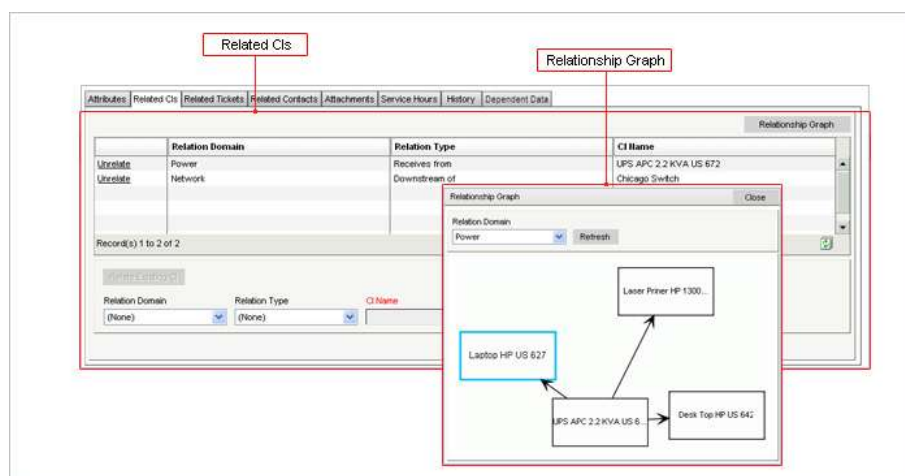
A CI record can be related to other Configuration Items in different relationship domains or be related to different contacts in different ways. As Application Administrator, you can create or modify these relationships as appropriate.

Related CI

The Related CIs tab allows you to relate other Configuration Items to the current CI record. You can choose a relationship domain as Logical, Network, Power, or Service. Depending on the Relationship Domain chosen, values available for Relationship Type change.

You can choose which CI you wish to relate from the Relate CI lookup. This is a mandatory field and you have to select a CI to relate to be able to relate the CI.

Multiple CIs can be related to each other in either the same domain or in different Relationship Domains. You can view the CI Relationship Graph in a specific relationship domain.



You can relate one Configuration Item to multiple CIs in different domains. However, the CI Relationship Graph depicts how the CIs are related to each other within one relationship domain only.

The relationship graph depicts multiple levels of relationships. This means that if a Configuration Item which is related to the current CI is related to other CIs (besides the current CI), then the Relationship Graph will also show this extended relationship. The level to which the relationship is displayed is controlled by a Configuration Parameter.

Related Contacts

A CI can have contacts or Support Groups related to it in different Relationship types, namely Owner, User, Support Provider, Change Approver and Change Reviewer.

Relating Contacts to the CI in appropriate Relation Type helps maintaining records about which contacts use or access a CI, and this can also be used for selecting Contextual Approvers or Reviewers for Change requests logged for a given CI.

Attributes Related CIs Related Tickets Related Contacts Attachments Service Hours History Dependent Data		
	Relation Type	Contact/Group Name
	Owner	Lien, Timothy
Unrelate	User	Goldratt, Ira
Unrelate	Support Provider	Adney, Amy

Record(s) 1 to 3 of 3

Relate Contact/Group

Relation Type: (None) Contact/Group Name: Admin, InteQ

If you have specified an Owner for the CI when creating or updating the CI record, the name of the contact will be displayed in the Related Contacts Tab. You can add other contacts or support groups to be related to the CI in other relationships.

Multiple contacts and/or support groups can be added as a Users, Change Approvers, Change Reviewers and Support Providers for the CI; but only one contact can be related to the CI as owner.

All CIs related to contacts get reflected in the Related CIs tab of the contact record. If a contact related to a CI is a Self-Service Users, he/she will be able to view and relate this CI to any Ticket they submit to support; this depends if this functionality is enabled for Self-Service Users via related Configuration Parameter.

Related Tickets

This tab displays all Tickets that have been logged for that particular CI record. When a Ticket is created, Configuration Items can be related to the ticket. If a particular CI record being viewed has been related to some tickets, these tickets will be automatically displayed in the Related Tickets Tab. You can view the Tickets, and access the ticket record from within the Related Tickets tab.

Related Attachment

You can relate attachments to a CI record to provide more information about the CI. You can choose to upload an existing attachment (from the Global Attachments) or choose a new attachment relevant to that CI record.

CI Service Hours

The Service Hour Tab on a CI record allows you to view and manage Schedules for a Configuration Item. You can configure multiple Schedules for a Configuration item like Service Availability Schedule or Outage/Maintenance Schedule.

The screenshot shows a software interface with a table of CI Relationships. A modal dialog titled 'Schedule' is open, allowing the user to define a new schedule. The dialog includes the following fields and options:

- Start On:** 02/03/2011
- End By:** (empty)
- Status:** Active
- Schedule Type:** Service Availability
- Start Time:** (empty)
- End Time:** (empty)
- Time Zone:** (GMT+00:00) Africa/Abidjan
- Repeat On:** All Days of the Week (checked), Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday (unchecked)
- Holiday List:** Baroda India 2010

Buttons at the top right of the dialog are 'Apply Changes' and 'Close'. A red box labeled 'Service Schedule' points to the 'Service Availability' option in the 'Schedule Type' dropdown.

To add a schedule for a CI, click on the Add Schedule Button. A Schedule form will be displayed in a new window. You can specify Schedule Start and End Dates, choose Schedule Type, specify Time-Zone when the schedule applies, define schedule applicability dates, and add a Holiday list to the schedule.

Attaching a Schedule to a CI helps in planning any downtime for a CI (for maintenance) and communicating the same to all Stakeholders, and also enables effective monitoring of SLA Compliance for CI availability.

Administering Configuration Management

The Configuration Management Module of Nimsoft Service Desk allows you to maintain a Configuration Items database. From this section, contacts (Service Desk Agents and Administrators) can view list of existing CI, create new CI, search for CI, and extract reports related to CIs.

You also have access to pre-configured Defined Searches, Reports and Dashboards. As Administrator, you have to manage access to these added features for other contacts (Service Desk Agents).

This section identifies Administrative decisions and actions you will take to allow Service Desk Agents and Self-Service Users to access Configuration Management.

Access and Permissions

Service Desk Agents ability to access the Configuration Management and all links under this module are managed by the Application Administrator. As the application administrator, you have to determine which aspects of Configuration Management are to be made available to contacts related to different Support Groups and Roles. The configuration Management Module contains four links:-

- List Configuration Items
- Create Configuration Items
- Search Configuration Items
- Reports

While you may want to allow Service Desk Agents involved in provisioning related activities the ability to Create New Configuration Items, you may want to restrict access to this link for Agents involved in Level 1 type of support. Similarly, you can decide to limit access to Configuration Item related Reports to just specific Support Groups who would need access to such reports.

You can manage the ability of Service Desk Agents to access these various links by enabling or disabling Permissions to the above links from the Manage Navigation Menu Option under Admin Utilities.

Defined Searches

Nimsoft Service Desk comes with a range of Defined Searches related to Configuration Management. As application Administrator, you can create new Defined Searches related to Configuration Items. However, not all Service Desk Agents would need access to all Defined Searches. As application administrator, you can control the ability of Service Desk Agents to access Defined Searches.

Defined Searches can be accessed from the Pre-defined Searches tab of the Search Configuration Item Link. A Service Desk Agents sees all Defined Searches, to which permission has been granted in this tab.

You can manage the ability of Service Desk Agents of different Support Groups and Roles to view and use the available Defined Searches by enabling or disabling Permissions to a defined search from the Permissions Tab of the defined search.

Reports

Nimsoft Service Desk allows you to access a range of reports related to Configuration Management. As Application Administrator, you can manage the ability of Service Desk Agents to view and access the reports link under Configuration Management and the ability of Agents to access each individual report.

A list of all reports to which the Service Desk Agent has been granted permission is listed in the Reports link under Configuration Management. Service Desk Agents can view the report, modify some of the data parameters, extract data into a CSV or PDF file, or print the report.

As application administrator, you can enable or disable access to the Reports Link from the Manage Navigation Menu link under Admin Utilities; and control access to individual reports from the Manage Report Configurations Link under Admin Utilities.

Dashboard

Nimsoft Service Desk allows you to view and manage access to the pre-defined Configuration Management Dashboard. You can also control access to any Dashboard that you have configured. You can control the ability of contacts related to different Support Groups or Roles to access the Dashboard.

You can enable or disable Permissions to the Dashboard from different Support Groups or roles by enabling or disabling access to the My Dashboard link via Manage Navigation Menu, and access to the dashboard via enabling permission to the Dashboard to Groups or Users.

Manage Related Config Parameters

You can manage Configuration Parameters to control the ability of Self-Service Users to relate Configuration Items to support tickets that they log and the display of CI relationships in the Relationship Graphs on a CI Record.

These functions are managed via changing the Values as appropriate under Manage Configuration Parameters.

How Do I

Below are some actions you can take related to Configuration Management.

Create or manage CI Attributes Template

You can configure a CI Attribute template for adding attributes to Configuration Items. The CI Attributes template gets applied to all CIs with related CCTI.

To configure a CI Attributes Template:

Step 1: Click on Manage CI Attributes Template under Application Setup.

All currently Active CI Attributes templates will be displayed in the list. You can view and modify an existing template or create a new template in the form below.

To create a new CI Attributes Template:

Step 2: Enter a Name for the CI Attribute Template, which is a required field.

You can provide additional information in the description field. However, you may choose to leave this field as blank because it is not mandatory to save the record.

Step 3: Click on Apply Changes to save the record.

By default, the status is set as Active. The template details like Created on, Created by, etc. will get updated automatically.

The Attributes section, from where you can relate attributes to the CI Attribute template, and the Related CCTI tab, now get activated. You can now add Attributes to the template.

In the Attributes Tab, a list of all Attributes that are currently related to the template get displayed. You can add Attributes from the form below.

Step 4: In the Attribute Name field, select an Attribute from the Attributes Name lookup. This list displays all Attributes in the Attribute Pool (created using Manage Attributes form).

When you select an Attribute, the related fields of Unit, Attribute Type and Possible Value (as relevant) will get automatically updated.

Step 5: If there is a default value that you wish to assign to the Attribute, you can specify the value in the Attribute Default Value field.

This value will be displayed as default value when the template is used.

Step 6: If you want the Attribute to be automatically added to a CI record to which the CI Attribute Template gets applied, check the Add During Creation Checkbox.

If this checkbox is unchecked, you can choose whether or not to apply the Attribute to the CI record, and manually apply the Attribute by using the Attach Attribute action.

Step 7: If you want the Attributes to be applied to existing CI records where the CI Attributes Template becomes applicable, you can check the Update Existing Configuration Items checkbox.

Step 8: You can check the Enforce Unique Value checkbox if you want the value applied to an Attribute to be unique. This is more relevant where the Attribute Value type is Text, Number etc., where you want to avoid duplicate values.

You can assign a Sort Order if needed; though this is not mandatory.

Step 9: Click on Save Attribute action button to add the Attribute to the Template.

The Attribute will get displayed in the table above. All Attributes chosen on the CI Attributes template will be displayed in the Alphabetic order (or Sort Order if defined) in the table.

CI Attributes templates get applied to a CI Record based on the CCTI of the CI record.

Step 10: Click on the Related CCTI tab. In this tab, you can relate the categorizations to which the CI Attribute template can get applied.

Step 11: In the form below, select Class (a required field), Category, Type, and Item to pull out the relevant Categorization Record.

Step 12: Click on Add CCTI to relate the categorization record to the CI Attribute template.

The template will now become available for all CI records with the same CCTI as the CI Attribute template.

Note: If you do not relate any CCTI to the CI Attribute Template, the Template will not get applied to any CI record.

Only those Attributes where the Add during Creation is checked will get applied automatically to the CI record with the record is created. All other attributes need to be manually attached as needed using the Attach Attributes action.

Create or manage CI records

You can create new CI records and modify existing CI records under Configuration Management Section of the Application.

To create new Configuration Item records:

Step 1: Click on the Create Configuration Item link under Configuration Management.

A blank CI record form will be displayed in a new window.

Step 2: Enter a Name for the Configuration Item in the Name field, which is a required field.

You can provide additional information in the Description field. However, as this is not mandatory, you can leave the field blank.

Step 3: In the Function field, you can specify the function, to indicate what the CI is used for. You can choose a function from the lookup or create a new function.

Step 4: If you follow a specific naming convention for Configuration Items in your organization, you can enter the CI tag in the Identifier field.

Step 5: Using the Search CCTI action button, search for a categorization that is to be applied to the Configuration Item. This is a required field.

Step 6: A Configuration Item has to be related to an Organization. You can relate the CI to an organization from the Organization lookup.

You can choose to further relate the CI to Site/location of the Organization; though this is not mandatory.

Step 7: You can relate the Configuration to contacts as Owner of the CI if necessary; though this is not mandatory.

Step 8: Click on Save option in the CI Toolbar menu.

The CI record will be created. CI ID, created date, etc. get automatically updated. The Attributes tab now gets activated and other tabs like Related CI, Related Tickets, Related Contacts, Attachments, Service Hours and History get enabled on the CI record.

The default Attributes of the Configuration Item records, and any Attributes added automatically from applicable CI Attributes templates get displayed in the Attributes table.

Step 9: Modify the Attribute value as appropriate for the CI record.

In the Template Name dropdown, you can view all CI Attribute Templates that get applied to the CI record based on matching CCTI.

Step 10: Select the CI Attribute Template from which you wish to apply attributes to the CI record.

Any Attributes applied during creation will be listed in the table.

Step 11: Click on Attach Attribute action button. Attributes Name lookup, containing Attributes from the CI Attribute Template will be displayed.

Step 12: Select the attribute from the Lookup.

The Attribute, with its default and set values will get added to the list. You can modify value as appropriate.

You can now relate the CI record to other CIs from the Related CI tab, relate the CI to contacts from the Contacts tab, relate an Attachment to the CI, or configure Service Hours for the CI, as required.

Note: CI records, with Categorization (CCTI), values for default attributes, Custom Attributes and relationship to related Contacts can be Bulk Uploaded in to the application once the relevant information is gathered in the appropriate format.

You can modify CI records as needed. All modifications will be displayed in the History Tab.

If the CI Record status is set as Deprovisioned, it will not be available for use in any transactions or relation to other entities in the application.

Relate a CI to other records

You can relate a Configuration Item (CI) record to other CI records and Contacts. You can relate Attachments to a CI and view information on all Tickets related to the CI from the CI record.

To relate a Configuration Item to other CIs:

Step 1: Click on the Related CI tab of the CI record. (This tab appears on the CI record after the record is first saved.)

Any CI records related to the CI will be displayed in the table.

Step 2: In the form below, choose a Relationship Domain. You can choose a domain as Logical, Power, Network or Service.

Step 3: Based on the Relationship Domain selected, you can choose the Relationship Type.

For example, if you choose Relationship Domain as Power, you can choose Relationship Type as Supplies to, Receives from or Related to.

Step 4: In the CI Name field, choose the CI you wish to relate to the current CI record. The lookup displays a list of all CI records belonging to the same Organization and with the same Categorization as the current CI.

You can choose to view all CI records that do not have matching CCTI and organization by selecting the View All Option.

Step 5: Click on the CI record that you wish to select the CI to be related.

Step 6: Click on Relate Existing CI action button, which now gets activated.

The CI will get related to the current CI and will be displayed in the table above.

You can view a Relationship Graph of related CIs in any one Relationship Domain at a time. A CI can be related to multiple CIs in more than one Relationship Domain.

A Configuration Item can be related to contacts and Support Groups. To relate a Configuration Item to Contacts/Support Groups:

Step 1: Click on the Related Contacts Tab of the CI record.

Any Contacts related to the CI will be displayed in the table. If you have assigned an Owner for the CI record, the Owner name will be listed in the table.

Step 2: Select a Relationship Type from the dropdown list.

You can relate a contact as User, Support Provider, Change Approver or Change Reviewer.

Step 3: In the Contact/Group Name field, click on the Lookup. The Name Search Lookup will be displayed. Select Contacts/Groups in the Show field to view either Contact names or Support Group names.

A list of Contacts/Support Groups will be displayed.

Step 4: Select the name of the Contact/Support Group to relate to the CI record.

Step 5: Click on the Related Contact/Group action button, which now gets activated.

The CI will get related to the chosen Contact/Group.

Note: If you don't select Relationship Domain, you will not be able to view the Relationship Graph for the related CIs.

The depth to which the Relationship hierarchy will be searched and displayed is controlled by Slice Parameter SCR_AFFECTED_SERVICES_SEARCH_DEPTH. If the value is set to 0, the entire relationship hierarchy will be traversed.

Associate a Schedule with a CI

To configure a schedule for a Support Group:

Step 1: Open the CI record for which you wish to configure the Schedule. If this is an existing CI record, you can pull out the record from List CI or Search CI options. If you are configuring a CI record, the Service Hours tab will get displayed after the CI record is saved.

Step 2: Click on the Service Hours tab.

If any schedule is associated to the Configuration Item record, it will be displayed in this tab.

Step 3: Click on the Add Schedule action button to open the Schedule lookup.

Step 4: Enter the Schedule Start Date, Start Time and End Time. All three fields are required fields. You can specify the end date if you want the schedule to be valid only for a specific duration.

A Schedule for a Configuration Item could be either Availability Schedule or Outage/Maintenance Schedule.

Step 5: The default Schedule Type is Service Availability. If you want to configure an Outage Schedule, select a Schedule Type as Outage/Maintenance.

Step 6: Select a time-zone from the dropdown list. This will be the time-zone for that schedule associated with the Support Group.

Step 7: Select days of the week that the schedule applies to.

Step 8: Relate a Holiday Group if the Schedule is to be excluded on holidays.

Step 9: Click on Apply Changes to create the new Schedule for the Configuration Item.

Note: If no schedule is associated with a Configuration Item, the default schedule is taken as 24 X 7.

Configuring schedules for Outage/Maintenance allows you to maintain outage related information on the CI record.

Availability Schedule information assists when SLA target is applied for Service Availability calculations.

Frequently Asked Questions

Some questions that you may have regarding Configuration Management and Manage CI Attribute Template are listed below:

Do I have to define CCTI for CI before I create CI records?

Yes, Categorization (CCTI) is a required field for configuring new CI records. Therefore, you have to create Categorization Records related to CI forms before creating CI records.

How does the status of a CI impact its availability for relationships with other records in the application?

The Status of a Configuration Item depicts which stage of the life-cycle the CI is at. When a CI is in Deprovisioned Status, it will not be available for relating with other CIs, tickets, and other records in Nimsoft Service Desk.

CIs in all other statuses will be available for relating to tickets, contacts, other CIs, and records.

Can Agents create new CI records or modify CI records?

Contacts designated as Service Desk Agents can create new CI records if they are assigned permission to access the Create Configuration Item link under Configuration Management.

The choice of allowing Service Desk Agents to create new CI records is up to the application administrator. Service Desk Agents can modify existing Configuration Item that they can access using the List CI or Search CI actions.

Can SSUs access and view CI records?

SSUs cannot view the detailed CI record. They can only view a listing of all those CI records that they are related to as Owner, User, Change Approver, Change Reviewer, etc.

They can relate the CI to a ticket that they log from the SSU interface if this feature is enabled for Self-Service Users (via Slice Parameter).

Can I delete a CI record? If yes, can I restore a deleted CI record?

When you delete a CI Record, the status of the CI gets set as Deprovisioned. The CI will then not be available for relating to tickets and other entities.

You can change the status of the Deprovisioned CI record to make it available again.

What entities can be related to a CI record?

A CI can be related to the following other records:

- Other CIs

- Contacts
- Tickets
- Knowledge Articles

What does the Service Hours of a CI record indicate- can I update multiple schedules for a CI?

The Service Hours of a CI indicates availability or non-availability time for a Configuration Item. This is particularly necessary for CIs categorized as Service as you can view Service Availability/Non Availability schedules.

You can configure multiple Schedules for a CI, for example, Availability Schedule, Outage, or Maintenance Schedule.

Can an item in the CI History tab be deleted or modified in any way?

The history tab of the CI record displays a list of all changes and modifications made to the CI.

This list gets automatically generated whenever there is a change in the CI record. You cannot delete or in any way modify the history record.

How does creating a CI Attribute Template help?

A CI form has a set of default attributes that are common for most CIs. These are captured by a default CI attribute template applicable to all CIs.

You may wish to add more attributes specific to the CI and CI management practices that you adopt in your organization. The CI Attribute template allows you to put together a list of attributes that can be applied to specific CI records. You can thus capture additional details over and above the data in the default CI attribute template.

Do I have to relate a CI Attribute Template to a CCTI? What happens if I do not associate the template to any CCTI?

Yes, you have to relate a CI Attribute Template to at least one CCTI. A CI Attribute template is configured for a particular Class of CIs. Therefore, if you don't relate a CCTI to a CI Attribute template, it will not be applied to any CI.

What happens if I add a new attribute to a CI Attribute Template - will it be automatically available for older CI records?

You can choose whether you wish to apply the new CI Attribute to older CI records or not. If you choose Update Existing option, the attribute becomes available on existing CI records as well.

What do the check boxes "Add During Creation" and "Update existing Configuration Items" mean? What is the implication of checking or not checking these?

When a CI attribute template is associated with a CCTI which has at least Category defined in addition to Class, the attributes are NOT applied to a CI (with the specified CCTI) automatically upon creation of a new CI.

The Check box for Add During Creation needs to be checked to apply the attribute during creation. If the check box is NOT selected, the attribute shall not be applied to new CI upon creation. It can be applied manually later at any time.

If the CI attribute template is associated with a CCTI that has only class defined, it applies to a new CI upon creation.

What does Enforce Unique Value mean? What is the implication of checking this checkbox?

If Enforce Unique Value flag is selected, each CI that belongs to the set of CIs to which the CI attribute template is applied to, must have a unique value. It is Unique Value across a set of CIs.

For example, default attribute template is applied to a set of CIs that includes "ALL CIs".

But a CI attribute template associated with a CCTI is applied to a "Set of CIs" that have the specified CCTI only. In this second case, the Uniqueness is verified only across the set of CIs to which the template gets applied on basis of CCTI (and not all CIs).

Enforcing unique values allows you to maintain those records where a unique values distinguishes one record from another.

If the enforce unique value is checked; when a user uses a value that is not unique, the user will get an error message stating that the field requires a unique value.

What happens if I delete an Attribute from a CI Attribute template? Will it impact older records?

You can delete an attribute from a CI Attribute template. On all older records where the attribute was applied, the value field and its associated value remains. However, the Attribute will get applied on any new records.

What happens if I delete/deactivate a CI Attribute Template? How does it impact older records?

The Inactive template will not be applied to new CIs that may be created. It will also not be available to older CI records when they are modified.

Can I add a new Attribute Name for a CI Attribute Template from within the same form?

Yes, you can add new Attributes to an existing CI Attribute template. Depending on the options chosen, the new attribute will be available for older records; or only for new records created going forward.

Can tickets and CIs have the same CCTI? Can one CCTI be associated with multiple forms?

Yes; tickets and Configuration Items (CIs) can have the same categorization. When configuring categorization, you can relate it to multiple forms including different ticket forms and CI forms.

Is it possible to use only three or fewer levels for categorization for a particular ticket or CI rather than using all four levels?

Yes; you can skip one or more level of categorization. You can choose to define only Class, only Class and Category, or only Class, Category and Type for a ticket or CI in Manage Categorization, and not define all levels.

However, please note that defining Class is required, while the remaining levels are optional. You can skip them the other three levels after Class is configured.

Is it possible to use only Class, Type and Item (and skip Category) in creating a categorization?

No, to define Type and Item, you have to define Category. This is because each level is incrementally related to the other. For a given class, there are certain categories; for a given class and category, there are specific types; and for a given class, category; and type, there could be items.

As the relationship is hierarchical in nature; you have to specify a higher level entity before specifying an entity lower in the hierarchy.

What is the effect on older records with a CCTI, when the CCTI is modified?

When an existing CCTI is modified, the old records (Tickets and CIs) to which it has been already applied are not updated. They continue with the CCTI as it was before modification. But new records can be linked only to the modified CCTI.

However, changing the CCTI after it is used as matching conditions for Action Options, Auto-Routes, SLA targets, etc., can lead to the entities not getting applied or progress of the ticket failing because a matching condition was changed.

What happens when a CCTI for a ticket or CI is made inactive?

The Ticket or CI record where CCTI was applied remains categorized as per the CCTI which is made Inactive. In its Inactive status the CCTI cannot be applied to new Ticket or CI records.

When an inactive CCTI is made active again, does it affect the CIs that have that CCTI?

When an Inactive CCTI is made active again, it becomes available for applying to new CI records or changing CCTI of existing CI Records. It does not impact CI records where it is already applied.

What happens to open ticket records when a ticket CCTI is made inactive?

Nothing changes for the Ticket. The Inactive CCTI is no longer available for applying to new tickets or changing the CCTI of existing tickets.

How do ticket templates with a particular CCTI get impacted when the CCTI is made inactive?

The Ticket Template continues to bear the Inactive CCTI. When a ticket is created from such a template, the Ticket also bears the Inactive CCTI.

Chapter 19: Knowledge Management

Overview

The Knowledge Management Module is a repository for building and maintaining a Knowledge Base for solutions to frequently occurring issues, answers to common queries from End Users, and other informative articles related to IT in the Organization.

The Knowledge Management Module is also used to publish information on Known Outages and News Articles visible on the Self-Service Users Interface.

Self Service Users can view Articles from the Knowledge Base Link under Support Services in the Navigation Menu. They also see News and Information on Known Outages in the Self-Service User interface of Nimsoft Service Desk.

This information is made available to Self-Service Users by the administrator from the Knowledge Management Module.

The screenshot displays the 'Knowledge Management' interface. It features a search section with a 'KB Article Category' dropdown, a text input for keywords, and 'View' and 'Clear' buttons. Below this is a 'Symptom Description' text area. Further down are four dropdown menus for 'Class', 'Category', 'Type', and 'Item', each with a 'Clear' button. The main section is a table titled 'List KB Articles' with columns: 'Short Symptom', 'Class', 'Category', 'Type', 'Item', and 'Sticky'. The table contains several rows of data, including symptoms like 'Message Not enough disk space displayed' and 'Black Berry will not synchronize'. At the bottom, it shows 'Record(s) 1 to 25 of 54'.

Short Symptom	Class	Category	Type	Item	Sticky
Message Not enough disk space displayed. Print file size ...	Desk Top Hard...	Peripherals	Hard Disk		No
Action options do not appear in appropriate menus in Infr...	Application	InfraDesk	Menus	Action Option	No
Adjacencies are not formed in OSPF (Open shortest path...	Networking	Routers	OSPF		No
AMD to Intro 45nm.Desktop CPUs in G3.					No
Black Berry will not synchronize	Application	E mail	Black Berry		No
Blackberry has a SMM ERROR.	Application	E mail	Black Berry		No
CAB file problem stops MS Office 20043 installation doe t...	Desk Top Softw...	Office Tools	MS Office	MS Office 2003	No
Cisco's home-network push.					No
Congratulations Tilol And may you climb from Peak to Peak!					Yes
Does my Password ever expire?					No

Service Desk Agents can search for solutions from a Ticket ; and use a solution presented in an Article to resolve the open ticket. They can also add solutions updated in the Solutions tab of a Ticket to the Knowledge Base, if this action is permitted by the Administrator.

The Application Administrator undertakes the task of creating KB Article Category, and creating new Knowledge Base Articles associated to a specific category.

Self-Service Users and Service Desk Agents can view Knowledge Base Articles that they have been granted Permissions to view. They can also rate a Knowledge Article , they can comment on whether the Article was useful in resolving their issue or not, and they can provide any other feedback about the Knowledge Article.

Besides providing a rating, Service Desk Agents can view the number of times a Knowledge Article was viewed; and how often it was useful in resolving an open issue. They can also view the comments and feedback provided by Self-Service Users and other Service Desk Agents about the Knowledge Article.

The Service Desk Agent submitting the article; or the administrator creating or approving the Knowledge Article can provide additional information by relating an Attachment to the article. This attachment can be viewed by Self-Service Users as well as Agents who have been granted permission to access the article.

All new Knowledge Base Articles, either added by Service Desk Agents from a Ticket , or created using the Create KB Articles link, remain in a Draft State . The application administrator (or a group or role designated for this task) can review the Knowledge Article, make any modifications required, and set the state as Approved. Once Approved, the KB Article will be available for other users.

Configurations related to the Knowledge Management Module, and activities related to maintaining the Knowledge Base are explained below.

Manage Knowledge Base Article

For Knowledge Base Articles to be available to Self-Service Users or Service Desk Agents, it is necessary to build a Knowledge Repository. Building the knowledge base involves two main activities - creating appropriate Category for Knowledge Articles and Creating new Knowledge Base Articles. These two activities are explained in detail below.

KB Article Category

Nimsoft Service Desk allows you to categorize Knowledge Base Articles. Categorization of a Knowledge Base Article helps in searching for solutions more effectively and in grouping all related articles under one category. Once a category has been configured, it can be applied to different Knowledge Base Articles that are created and saved in the Knowledge Base.

You can also create Custom Categories when you are creating a new Knowledge Base Article.

Manage KB Article Category

You can create new KB Article Category from the Manage KB Article Category link under Knowledge Management. This link displays the KB Article Category form. You can view a list of existing KB Article Categories in the table; clicking a category displays the category details. You can filter the list to manage the items listed in the table.

Nimsoft Service Desk provides System-Defined categories which can be used to publish information on the Self-Service User interface. The System-defined categories of News, FAQ, and Outage allow you to publish relevant details in the Self-Service User Interface.

You can choose whether this information is to be published on the Self-Service User Interface or not by checking or un-checking the Show on Knowledgebase Home checkbox.

You can create new KB Article Categories or modify existing KB Article Categories from the KB Article Category Form. If you create a KB Article Category from within this link; it will be marked as Pre-Defined.

You can also choose whether articles related to this category should appear on the Knowledge Base page in the Self-Service User Interface or not. If the 'Show on Knowledgebase Home' check box is checked, the articles related to this category will be listed in the Recently Modified Articles list on the Knowledge Base home page on the Self-Service User interface.

Custom Categories

You can also create new Custom KB Article Categories from within the Create KB Article form. When you create a new Knowledge Article , you have to associate a category for the article. While selecting a category; if you choose the category “Custom” from the lookup, you will be asked to enter a Custom Category Name (this is a mandatory field). The new category you add in this field can be seen in the KB Articles Category List.

You can manage the status of a KB Article (Active/Inactive). However, you cannot modify the status of the System-Defined categories or make any other changes to these categories. You can only view details of these categories.

Create KB Articles

You can create new KB Articles from the Create KB Article link. Clicking on this link displays a blank KB Article form. You can choose an appropriate category for the KB Article; choose CCTI for the article, provide the mandatory information on Short Symptom, and other relevant information like Symptom Description , Cause and Resolution , and save the KB Article.

The screenshot shows the 'KB Article Details' form. Annotations include:

- KB Article Specifications:** Points to the top section of the form containing fields for 'Related To KB Article Category', 'Custom Category Name', 'Short Symptom', and a 'Sticky KB Article' checkbox.
- Further Information Tabs:** Points to the bottom section of the form containing tabs for 'Details', 'Keywords', 'Feedbacks', 'Related Items', 'Attachments', and 'Permissions'. The 'Details' tab is active, showing 'Symptom Description', 'Cause', and 'Resolution' text areas.
- KB Article Details:** Points to the top right section of the form containing fields for 'KBID', 'Average Rating', 'Status', 'Created On', 'Created By', 'Last Approved', 'Approved By', 'Last Modified', and 'Modified By'.
- Rating:** Points to the 'Average Rating' field.
- State:** Points to the 'Status' field.

Class	Category	Type	Item
Desk Top Hardware	Peripherals	Mouse	Logitech

Number of Times Viewed	Number of Times This Article Solved an Issue
0	0

Created On	Created By
30/07/2008 07:47:49 PM	Admin, Intel

Last Approved	Approved By
30/07/2008 07:47:49 PM	Admin, Intel

Last Modified	Modified By
30/07/2008 07:47:49 PM	Admin, Intel

Once the Article is saved, additional tabs of Keywords , Feedbacks, Related Items, Attachments , and Permissions will be displayed. You can choose to add appropriate details on relations into the relevant tabs.

Keywords

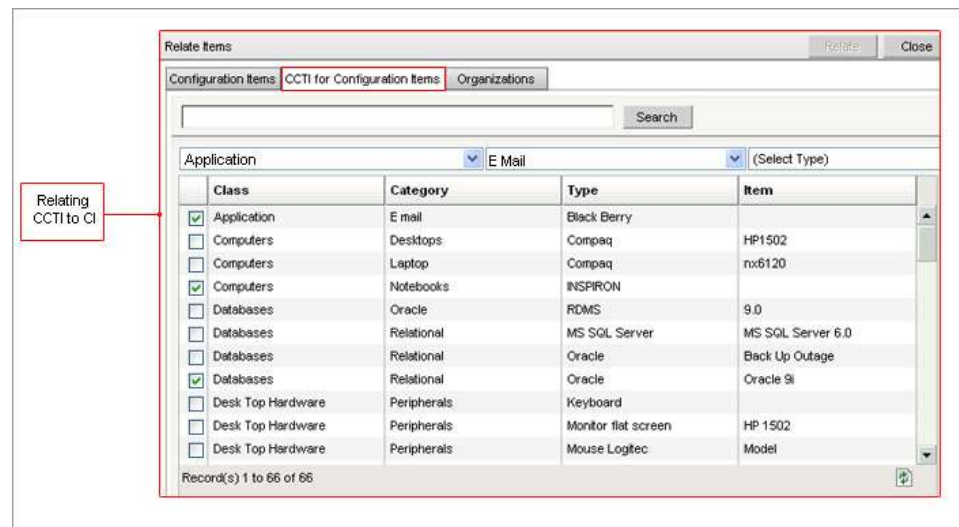
Keywords from the Short Symptom field get automatically picked and displayed in the Keywords table. You can choose to add more keywords to the list to broaden the scope of the KB Article and ensure that the KB Article will be displayed during a Keyword search; when the keywords match the requirements.

All Keywords that are manually added can be modified or deleted; however, keywords that are automatically picked cannot be edited or removed.

Relate KB Articles

You can relate the KB Article various entities like Configuration Items , CCTI of Configuration Items, and Organization (site and location). Adding appropriate relationships ensures that search for knowledge Articles is appropriately filtered and thereby more effective.

These additional filters are useful when a Service Desk Agent is attempting to search for a Solution for a ticket, as the Agent can use these filters when identifying the best available solution for an open Ticket .



Relate Attachments

Files with useful information can be related to a Knowledge Article for reference. The Attachment Tab provides ability to “Add New” and “Relate Existing”.

The New Attachment can be added and specified as Global to make it available for attaching to other records. The File added as an Attachment can be unrelated.

External Links (URL) can also be related as Attachment as a “Document Link”.

The Attachment added is listed in the Attachment Tab.

While adding an attachment specific File Formats are permitted.

File Type	Description
Compressed (*.zip, *.gz, *.rar, *.tar, *.jar)	Compressed files can be attached and viewed by suitable tools that decompress
Document Link	Links to external URL can be attached and accessed
Executable (*.exe, *.bat, *.com)	Executable code files can be attached
Image (*.bmp, *.gif, *.jpeg, *.png, *.gif)	Image files can be attached and viewed by suitable tool
Mail Message (*.msg)	E-Mail messages can be attached and viewed
Office Documents (*.doc, *.rtf, *.ppt, *.xls)	MS Office files can be attached and viewed
Other Files (*.*)	Files of other formats can be attached
Portable Documents (*.pdf, *.ps)	Portable files can be attached and viewed
System / Application Logs (*.log)	Logs files can be attached
Text (*.txt, *.csv, *.dat, *.sql)	Text documents can be attached and viewed
Web (*.css, *.htm, *.html, *.js)	Web pages can be attached and viewed

Knowledge Management Functionality

The Knowledge Management module allows you to make Knowledge Articles available to Self-Service Users and Service Desk Agents in different ways. This section explains the functionality offered by Knowledge Management module and how you can optimally use this module to manage the Knowledge Base for your instance of the application.

Rating and Feedback on Knowledge Articles

The Knowledge Management Module enables collection of three types of data related to the Knowledge Article. All these inputs act as measures to analyze how useful a Knowledge Article has been.

The screenshot displays the 'Feedbacks' tab of a Knowledge Article interface. At the top, there are tabs for 'Details', 'Keywords', 'Feedbacks', 'Related Items', 'Attachments', and 'Permissions'. Below these, the 'Rate This Article' section includes a 5-point rating scale (radio buttons 1-5) and a question 'Does this article solve your problem?' with options 'Yes', 'No', and 'I don't know'. A 'Submit' button is located to the right. Below the rating section is a 'Comments' text area with a 'Submit' button. At the bottom, a table titled 'Feedback Received' shows the following data:

Date	User	Rating	Solved?	Comments
25/01/2011 06:23:41 PM	Dalglish, Sam ITS11	3	I don't know	Some of the details are too technical

Below the table, it indicates 'Record(s) 1 to 1 of 1'.

The parameters that can be measured are:-

- Number of times a KB Article has been viewed or accessed by users: This counts the number of visits by the user to the KB article through a ticket based search solution and excludes all other access.
- Number of times a KB Article Solved a user issue: A user can provide this rating by selecting whether a KB Article was useful in solving the issue or not.
- Average Rating given by users to a KB Article: This permits a user to rate the article ONCE. It gives input to calculate the Average Rating of the KB article based on all user input to the date. The average rating could reflect the intrinsic value, quality, and clarity of contents as perceived by the user.

Both Self-Service Users and Service Desk Agents can comment on the usefulness of the Knowledge Article, rate the article, and comment on the article.

While Self-Service Users cannot view the feedback submitted, they can view the Average Rating on a Knowledge Article. Service Desk Agents can view the average rating, view the counters for number of times a Knowledge Article has been viewed, and the feedback submitted by other contacts.

As Application Administrator you can use data generated by the counters and feedback to analyze a knowledge article and make modifications to it as required. You can also view a report related to Knowledge Articles, and decide how to better manage the Knowledge Base.

KB Articles for Self-Service User Interface

Self-Service Users of Nimsoft Service Desk can view News, Frequently Asked Questions, and information on Known Outages if this information is published and made available to the Self-Service User group.

The Self Service User interface has a section in the Navigation Menu called Support Services, with links to New, FAQs, Knowledge Base, and Known Outages.

Publishing Known Outages allows Self-Service Users to be able to plan their work better; especially if an outage is likely to lead to disruption in an available service that they access.

FAQ items can be used by Self-Service Users to find response to queries related to the IT Services they use, thus reducing the dependence on support. News and other informative articles can be used to publish information relevant or useful for Self-Service Users.

You can also control the content visible in the Knowledge Base link in the Self-Service User interface by managing visibility of this category and related articles by checking on the Show on Knowledgebase Home checkbox. Articles created under these categories will be displayed in the Knowledge Base link on the SSU Interface.

The screenshot displays the Knowledge Base interface with the following sections:

- Search Filters:** A box at the top containing search filters for Keywords, Category, Classification, and Modified Date From/To.
- Knowledge Base:** A section with search filters and a list of articles.
 - Recently Modified Articles:**
 - Testing the system to see whether Self-Service Users are able to access articles related to this category. Last Modified: 03/03/2011
 - Testing for Outage information general by InnaDesk admin. Last Modified: 12/15/2010
 - What is Log Shipping? Last Modified: 06/03/2010
 - Earned Leave for the people working on shifts. Last Modified: 05/26/2010
 - Network service outage. Last Modified: 05/25/2010
 - Informative Articles:**
 - Large Attachments with E Mails received / sent through MS Outlook. Last Modified: 05/20/2010
 - The Ways To Keep Your Laptop Battery Alive. Last Modified: 05/18/2010
 - How to Reset Your Printer? Troubleshooting for Resetting Your Hp, Dell, Lexmark, Brother or Samsung Printers. Last Modified: 05/18/2010
 - What is Log Shipping? Last Modified: 06/03/2010
- KB News / Information:**
 - Mr. Norman Proudhurst to join the General IT Support Group, at US HQ. Last Modified: 05/18/2010
 - Earned Leave for the people working on shifts. Last Modified: 05/26/2010
 - News:**
 - Congratulations T&F And may you climb from Peak to Peak ! Last Modified: 05/18/2010
 - TVPS tags the Innovator of the Year Award for 2009. Last Modified: 05/18/2010
 - Latest HP Notebook Grows Up, Stays Mini. Last Modified: 01/06/2009
 - Cisco's home-network push. Last Modified: 01/06/2009
 - HP to showcase Firefly Gaming Notebook with Dual-Screen and MALL. Last Modified: 01/06/2009
 - Testing Access:**
 - Testing the system to see whether Self-Service Users are able to access articles related to this category. Last Modified: 03/03/2011

There are three System Defined KB Article Categories - News, FAQs and Outages. You can use these categories to publish relevant content for the Self-Service User Interface.

When creating the content under these categories, only content in the Symptom Details and Symptom Description gets displayed. Any detail entered in the Cause and Resolution fields does not get displayed on the Self-Service Interface.

To allow the Self-Service Users to view these articles, you have to enable permissions to the article from the Permissions Tab of the KB Article.

Search Solutions Functionality

The Knowledge Management Module is designed to store solutions to known issues, work-around to common incidents, response to common queries, and to store other information of use or interest to those who access Nimsoft Service Desk.

The purpose of maintaining a Knowledge Base is to provide users a repository of solutions that they can use to solve an issue they are facing with an IT object or service.

Users can look through the Knowledge Base to find solutions to an issue they are currently facing and apply that solution to resolve the current issue. This saves time and effort in working on an issue which has a known solution.

Service Desk Agents working on Tickets can search through existing Knowledge Base Articles for solutions to open tickets from within the ticket. They can also view solution details from a recently resolved ticket, if this feature is enabled.

If a solution from a Knowledge Base Article or a recently resolved ticket is useful in resolving the current issue, they can select the solution or ticket; and Cause and

Resolution details from the KB Article or recently resolved Ticket get copied on to the appropriate fields on the open ticket. The KB Article ID or Ticket ID gets populated into the relevant field on the open ticket.

When Service Desk Agents use the 'Search Solution' Action button on the ticket's General Information Tab, a Search for Knowledge Articles Lookup is displayed. This Look-Up displays Two check boxes: Include KB Articles and Include Recently Resolved Tickets.

They can choose either or both of the check-boxes depending on whether they want to expand or restrict the search.

They can also use additional filters of related Configuration Items, CCTI of CI or Organization to better manage their search. By setting up effective relationships of Configuration Item, CCTI of CI and Organization, you can enhance the effectiveness of a search for solutions from a Ticket .

As application administrator, you can manage the ability of Service Desk Agents to use Recently Resolved Tickets in resolving open tickets by managing the relevant Configuration Parameter. This parameter also allows you to manage the period till when solutions from resolved tickets can be displayed.

Administering Knowledge Management

As application administrator, you can manage how Self-Service Users and Service Desk Agents access the Knowledge Management Module and the related functionality. This section details the tasks done to manage Knowledge Management module.

Access and Permissions

As application administrator, you can control access of users to Knowledge Base Articles by assigning Permissions to different users or groups from the permissions tab of the Knowledge Base Article. From this tab, you can add or remove permissions to view the article for contacts, support groups, or roles.

You can also control the ability of Self-Service Users to see a particular Knowledge Base Article in the Knowledge Base Home page on the SSU Interface.

A contact can view only those solutions that he/she is permitted to view. If Permissions are not granted, the article will not show up even if it matches a Global Search of advanced search parameter.

You can also manage the ability of Service Desk Agents to add solutions from a Ticket to the Knowledge Base by managing the Ticket Toolbar to control access to this function. Further, you can manage the ability of Self-Service Users and Service Desk Agents to view the different links related to Knowledge Management in the Navigation Menu.

By enabling or disabling access to a link in the Navigation Menu from the Manage Navigation Menu option, you can control what the user sees and does related to Knowledge Management.

Knowledge Management Reports

As Application Administrator, you can access the “ Knowledge Article By Categories” Report related to the Knowledge Management Module.

You can use this report to view the results of the feedback received from the users and to drill down to its details. The report gives complete data accumulated for the KB article as well as data of a selected period.

You can use these reports to manage the Knowledge Base more effectively. You can determine whether or not access to the report is to be given to Service Desk Agents. Data from this report can be used to better manage the Knowledge base; and enhance the solutions and articles available in the Knowledge Base.

Manage Related Config Parameters

There are different Config Parameters that control the Knowledge Management related functions for Self-Service Users and Service Desk Agents.

As application administrator, you can decide whether Self-Service Users can view Solutions Details on tickets or not.

Depending on the value set on this parameter, Self-Service Users will be able to view solution details on resolved tickets. You can also control the maximum number of entries that will be listed per page in a Search Solution action on the Self-Service User interface.

To manage the search solution functionality for Service Desk Agents, you can enable or disable the ability of Service Desk Agents to view Recently Resolved Tickets when searching for solutions. By setting an appropriate parameter value, you can control whether or not recently resolved tickets can be seen and used to resolve tickets.

How Do I

Below are some actions you can take related to Knowledge Articles.

Create or Manage Knowledge Articles

You can create Knowledge Articles from the Create KB Article link under Knowledge Management. Service Desk Agents can also create new Knowledge Articles by adding solutions from a ticket they are working on, if this action is enabled for them.

To create new Knowledge Articles from within Knowledge Management:

Step 1: Click on the Create KB Article link in the Knowledge Management Module.

A blank Knowledge Article form will be displayed in a new window.

Step 2: Select a KB Article Category from the lookup. This is a required field, and you cannot leave it blank.

A list of available KB Article Categories will be displayed in the lookup.

If you choose KB Article Category as Custom, the Custom Category Name field will be enabled and will be shown as Required field. You can type in a new category in this field.

Step 3: In the Short Symptom field, enter a brief description about what the Article is about. For example, if the Article is a solution to a known issue, you can enter the brief symptom description in this field.

Step 4: Select a CCTI from the lookup to relate the Knowledge Article to ticket CCTI if appropriate. This helps when Service Desk Agents search for Solution from the ticket. KB Articles with the same CCTI will be displayed in the search result.

Step 5: Enter further information related to the Knowledge Article; i.e. Symptom, Cause, and Resolution details.

Step 6 Click on Save to save the Knowledge Base Article.

Once the Article is saved, the other tabs, such as Keywords, Feedback, Related Items, Attachments, and Permissions get enabled on the Article form.

Step 7: In the Keyword tab, add any Keywords you wish to manually add to the list. A set of keywords gets automatically identified and listed by the system. You may add more if necessary.

Step 8: From the Related Items tab, relate the article to other entities like Configuration Items, CCTI of CI and Organization if necessary.

Step 9: From the Attachments tab, relate any attachment to the Article if required.

Step 10: You can assign permission to access the knowledge article for Users, Support Groups and Roles.

When Service Desk Agents add Knowledge Articles from the ticket (using the Add to Knowledgebase menu item on the Ticket Toolbar):

- The Ticket Description gets automatically included in the Symptom Description field,
- Ticket details gets updated in the Symptom field
- Cause and Resolution details from the Solutions tab get updated in the Cause and Resolution field.
- Ticket CCTI gets related to the CCTI field.

Agents can just choose the KB Article Category, provide any other necessary information and save the record.

Note: All new Knowledge Articles are in Draft State (including articles created from Knowledge Management Module). You have to set the state as Approved for the Article to be available for users with Permission enabled.

Only those Articles that are in Approved State and Active Status will be available for viewing and other transactions. Access is also controlled by permissions.

The ability of Service Desk Agents to Add solutions to Knowledgebase can be controlled by enabling or disabling access to the Add to Knowledge base menu item on the Ticket Toolbar. You can manage permissions from the Manage Toolbars link under Administration Utilities.

Relate a KB Article to other records

You can relate a Knowledge Base Article to other records like Configuration Item, CCTI of Configuration Items, and Organizations. You can also relate attachments to a Knowledge Article.

To relate a Knowledge Base Article to other records:

Step 1: Open the Knowledge Base Article to which you would like to relate other records.

If you wish to relate records to an existing Knowledge Base Article, you can search the Article from the List of KB Articles page. If you wish to relate records to a newly configured Article, the Related Items tab will get displayed on the Article record after the Knowledge Article is saved.

Step 2: Click on the Related Items tab.

If any items have been related to the article, these will be listed in the form. You can relate new items from this tab.

Step 3: Click on the Relate Item action button.

A Relate Items lookup will open in a new window. This form has three tabs - Configuration Items, CCTI of Configuration Items, and Organizations.

Step 4: Choose what record you wish to relate and select the record from the list below.

Step 5: Click on Relate after you have chosen the records you wish to relate.

You can choose multiple records from each tab to relate more than one record at a time. The lookup will close automatically, and the related items will be listed in the form. You can unrelate any record by clicking on the Unrelate action.

Note: Service Desk Agents can use these relationships to get a more filtered output when searching for solutions. The Search Solutions lookup has filters, where the agent can filter the search to include only records with matching Configuration Items, CCTI of CI, or Organizations.

Manage News, FAQs and Known Outage related information available for SSUs

As Application Administrator, you can create and Publish New Articles, FAQs and information on Self-Service User Interface.

You can create new articles from the Create KB Article link under Knowledge Management.

Step 1: Click on the Create KB Article link under Knowledge Management to view the blank KB Article form.

Step 2: From the KB Article Category list, choose category News/FAQ/Outage depending on the type of article you wish to configure.

Step 3: Enter required details in the Short Symptom field.

You need not relate the article to any CCTI as this is not relevant to the category chosen.

Step 4: In the Symptom field, provide additional information about the article.

The Short Symptom field will be displayed as Article title in the Self-Service Interface. The Symptom will be displayed in the details section when the article is viewed.

You need to enter any information into the Cause and Resolution field as these fields will not be displayed when the article is categorized as New/FAQ/Outage.

Step 5: Click on Save to save the new article.

All other tabs will get displayed on the record. You need to associate any relations as this is irrelevant to the chosen categories.

Step 6: From the Permissions tab, assign permission for access to the Article. You can grant permission to the Self-Service Group, thus enabling access for all Self-Service Users.

You can also assign access to Service Desk Agents or other groups if needed. If permitted, Agents will be able to search for the Article and view it in the list.

Note: Ability of Self-Service Users to view Knowledge Base section, News, FAQs and Known Outages can be controlled by enabling or disabling permissions to these links in the Navigation Menu of the Self-Service User Interface. You can do this from Manage Navigation Menu link under Administration Utilities.

Enable Agents to use Recently Resolved Tickets for Solution to Open Tickets

You can enable Service Desk Agents working on Tickets to find and use Solution Details from recently resolved tickets to solve open tickets. To enable this feature:

Step 1: Click on the Manage Slice Configuration link under Application Setup. A list of all Slice Configuration Parameters will be listed.

Step 2: Filter the list by selecting Parameter Category 'Knowledge Management', and click on Refresh.

The list will be refreshed and only those Parameter Categories relevant to Knowledge Management will be listed.

Step 3: Click on Parameter Name
KB_ARTICLE_SEARCH_INCLUDE_TICKETS_RESOLVED_WITHIN_PERIOD.

The parameter details will be displayed in the form below.

Step 4: In the Parameter Value section, click on the radio button to choose from the options provided.

You can choose from None, 30 days, 90 days, 180 days, and 360 days.

The default value is set as None; meaning that the ability for Service Desk Agents to view and use Resolved Tickets when using Search Solution functionality will not be enabled.

Note: Enabling this feature allows Service Desk Agents to broaden their search for a ticket solution. Service Desk Agents can choose to expand the search result by checking on the Include Recently Resolved Tickets checkbox.

Only those tickets where Cause and Resolution details have been provided before the ticket is resolved will be displayed if Service Desk Agents choose to include recently resolved tickets when using Search Solution functionality.

Frequently Asked Questions

Below are answers to some questions related to Knowledge Management.

Will Self-Service Users be able to view Knowledge Articles? Can this be controlled?

You can control access to Knowledge Articles by enabling or disabling permissions for user, support, and roles. A Self-Service User will be able to view all those Knowledge Articles that they have permission to view.

You can also control the user's ability to view Knowledge Base link and access actions related to Knowledge Management by controlling permissions.

Do I have to create KB Articles Category before I create KB Articles?

KB Article Category is a required field for creating KB Articles. It is therefore advisable to configure a KB Article Category before creating a KB Article.

You can also create new KB Article Category from the Create KB Article page itself by selecting KB Article Category as Custom.

Which KB Articles are displayed in the Knowledge Base section of the Self-Service User interface?

You can determine which articles get displayed in the Knowledge Base section in the Self-Service User Interface. This can be managed by checking the Show on Knowledgebase Home checkbox for a specific KB Article Category.

All articles related to a KB category, where the Show on Knowledgebase Home is checked, will be listed in the Knowledge Base section under this category name.

What does the Custom Category Name indicate - why is the field showing as Required Field when I choose category as Custom?

If the KB Article you propose to create does not fit into any category, you can create a Custom Category from the Create KB Article form. To do so, you can choose the KB Article Category as Custom.

Thus, only when the Category is Custom, the Custom Category Name field will be enabled and it will be enabled as a required field.

How do the counters for Number of Times Viewed and Number of Times This Article Solved an Issue get updated?

The Counters for Number of times viewed gets updated every time the KB Article is accessed by a logged in user.

The counter for Number of times the Article solved an issue gets updated when a logged in user provides feedback that the article solved the issue by selecting yes for the question Does this article solve your problem.

What are the items that a KB Article can be related to?

A KB Article can be related to Configuration Items, CCTI of Configuration Items, Organization, Site, and Location.

Relating a KB Article helps in narrowing search for solutions for an open ticket. When Service Desk Agents attempt to Search for Solution to a ticket, they can filter the search using the above parameters to get a better search output.

What does the Draft or Approved State of a KB Article indicate? Can a KB Article be directly approved without going into Draft state?

All new Knowledge Articles are in a Draft State. This state indicates that the KB Articles is new and has not been reviewed. Knowledge Articles in a draft state will not be available for viewing in the Searches and other lists.

Upon review, you can set a Knowledge Article as Approved. Once approved, the Knowledge Article will be available to all those users who have been given permission to access it.

You cannot move a Knowledge Article directly into Approved State.

Can I control ability of only agents from particular groups to Add items to the Knowledgebase?

Yes, you can control ability of users or support groups to add articles to the Knowledgebase. You can enable permission to Add to Knowledgebase on the ticket toolbar to only those users, support groups, or roles as required.

Can Agents or Administrator manually add key words to a KB Article?

Yes, Service Desk Agents and Administrators can manually add key words to the KB article. All manually added Key Words can also be deleted.

Will Agents be able to see items like FAQ, Known Outage and News related KB Articles?

While the items like FAQ, Known Outage, and News related KB articles are intended for display in the Self-Service User interface under respective sections; Service Desk Agents can view these articles if they have been given permission to the KB Article record.

If permission is enabled, agents will be able to see these articles by searching for KB articles related to the above categories.

Can Agents access reports related to Knowledge Management?

Access to Knowledge Management related reports is controlled by Permissions. Permission to access the report can be granted to selected users, support groups, and roles.

Chapter 20: Manage Ticket Modules

Overview

Ticketing is at the core of Service Desk operations. All requests from the end-users of IT Support, reported either via the web (Self-Service User Interface), email, phone, or as a walk-in are logged as a Ticket in Nimsoft Service Desk.

These Tickets are then assigned to Service Desk Agents who work towards providing a solution to the request raised. Any update on tasks done towards resolving the request can also be maintained as a worklog in the ticket itself.

There are five core Ticket modules in Nimsoft Service Desk.

- Request Management
- Incident Management
- Problem Management
- Change Management
- Task Management

Each Ticket module allows Users to log tickets, view Ticket Lists, search for tickets, and extract reports related to tickets. A detailed explanation on the features of each ticket modules, functionality specific to that module, and how the modules are used by Agents (depending on how the module is configured) is explained in the Agent User Section of the guide.

A Ticket can be related to other tickets, one ticket can be a child to another ticket - giving the ticket a Parent Child relationship. An Incident or Problem Ticket can be classified as Global Issue and other tickets can be related to this Global Issue. Action on a Parent Ticket can be carried forward into the Child Ticket.

As the Application Administrator, you can manage various aspects of ticket functionality for the Self-Service Users and Service Desk Agents. These include defining CCTI for tickets, enable time tracking on the ticket, setting up custom fields for tickets besides defining the ticket Workflow Actions for a ticket.

Functionality such as default assignment of the ticket to a chosen default support group, control of the Status at which tickets can't be modified, etc., can be managed by setting appropriate Values in the Configuration Parameters related to that ticket.

This section discusses the various actions the Nimsoft Service Desk Application Administrator, will take to set up generic ticketing functionality. The processing of a Ticket through its life-cycle based on Workflow configurations are dealt separately under Manage Workflow Tools section.

Setting Up Tickets

While a default ticketing functionality is built into Nimsoft Service Desk, you will be required to set up Categorization for tickets for the ticketing function to be more effective and organized. Similarly, you may wish to manage the Ticket Toolbar options available to Service Desk Agents depending on the Support Group they belong to or the actions they take.

You can also modify value options of fields like impact, priority, urgency, etc. This section identifies the various actions you will take to set up the basic ticketing functionality as per your needs.

Manage Categorization

Categorizing Tickets helps set up effective auto-routes based on the type of request that is being logged. It also helps find appropriate solutions to an open ticket by searching for Knowledge Base Article and Resolved tickets with same Categorization .

For example, you can create a Categorization with Class - Server, Category- Exchange Server, and relate the Categorization Record to Change Tickets, Service Requests, Incident Tickets, and Problem Tickets.

You can then set up an auto-route that routes tickets with a specified categorization to be assigned directly to a specific support group. Thus tickets with a specified Categorization bypass the default assignment group and can be worked upon directly by members of a specialized group.

Categorization Lookup for Service Desk Agents:

A categorization record becomes available on all tickets that are related to record. When Service Desk Agents log a ticket, all Categorizations that are applicable to that ticket type get displayed in the Categorization look up that is displayed when they click the search CCTI action button on the ticket form.

When setting up a Workflow Action, like Accept Assignment on a ticket, you can also mark Categorization as a required field. This way you can ensure that all tickets are appropriately categorized.

Categorization by Self-Service Users: Self-Service Users can also categorize tickets when they submit a ticket. Self-Service Users see a 'Type' field on the ticket. It displays a dropdown list of all available classes by which they can classify the ticket.

You can disable Categorization of tickets by Self-Service Users by hiding the Type field on the ticket form on the Self-Service User Interface. This can be managed by Configuration Parameters SSU_HIDE_REQUEST_FIELD. The fields you can hide are

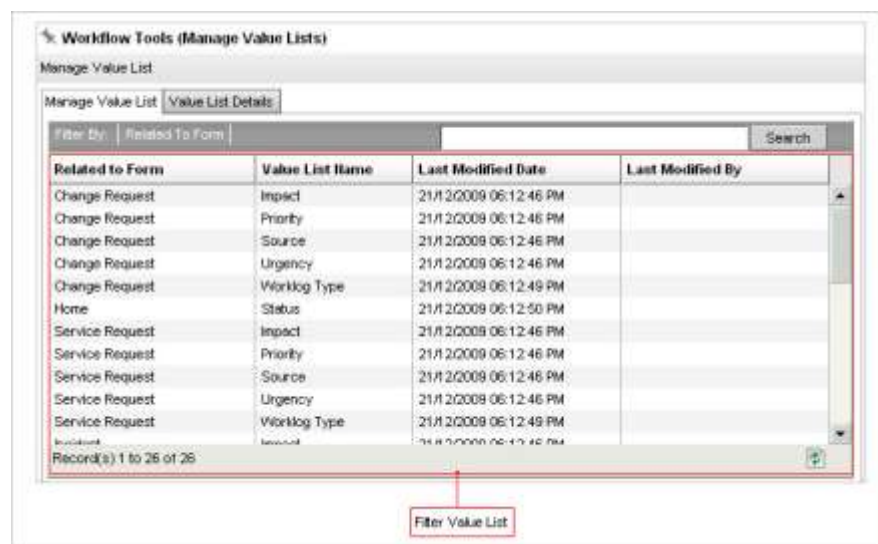
Priority, Urgency, and Type. If you check the field 'Type', then Categorization by Self-Service Users gets disabled.

Manage Value Lists

Ticket fields like Source, Priority, Urgency, Impact, and Severity have specific pre-defined Values in Nimsoft Service Desk. The Value in these fields can be used in Auto-Routes, workflow configurations, searches, etc.

Nimsoft Service Desk allows you to modify the Value options and highlighting a ticket in the Ticket List based on the value as per your naming conventions and preferences. For example, while some organizations may refer to Priority of a Ticket as High, Medium or Low another organization could prefer Priority Level 1, Level 2, or Level 3.

To enable your Users (Service Desk Agents and Self-Service Users) to use values they are familiar with for items on the ticket field, Nimsoft Service Desk allows you to manage value lists to change available value options for a specified set of fields.



You can Manage Values from the Manage Value Lists link under workflow tools. Clicking on this link will display the Value Lists Table, where a set of attributes with pre-defined values is listed. Clicking on an item in the list displays the details of the attribute and its predefined Values in the next tab.

Add or Modify Values:

The value options are editable, you can replace the pre-defined values with your custom values. For example, you can modify the value of Impact from the default High, Medium, Low to Severe, Medium, and Minor.

You can use these Values when configuring Auto-Routes, SLA calculations, and any

other feature where the Impact field is used in a ticket action configuration.

Modify Highlighting:

The application also allows Highlighting of columns based on the value of these fields. When modifying Value lists, you can also change the column highlight color to a color of your choice from among the available options. The changes take effect immediately; and will be available to you for the next transactions.

Note: Value options for fields like Status and Worklog Type cannot be changed. You can only change the Sort Order and choose highlighting for these fields.

Modifying Value Options enables you to retain the field naming conventions that your Users are familiar with; thus enhancing user experience.

Manage Ticket Toolbar Options

Ticket forms, Configuration Items form, and Knowledge Article have a toolbar option that allows the Users to take certain actions on the form. A standard set of toolbar options are available on these forms. Depending on the nature of Tasks a Service Desk Agent handles in your Organization, you may want to restrict the actions available for an agent.

Manage Toolbar Options allows you to manage Permissions for the Toolbar options for different users, Support Groups, and Roles. By not granting permission for an item on the toolbar; you can control the ability of the user to view and therefore execute that action.

You can control Toolbar Options from the Manage Toolbar Options link under Admin Utilities. Clicking on this link displays the Toolbar Options form.

Administration Utilities (Manage Toolbars)

Filter By: Form Type Search

ID	Toolbar Name	Toolbar Item	Toolbar Code	Sort Order
119	Save	Save	save();return;	200
96	Create New	Create New	resetform();return;	100
85	Manage Global Issue	Relate to a Global Is...	if(document.getElementById("this_ticket_is")[0].checked){alert("\$(@ms...	802
99	Delete	Delete	if(confirm("\$(@msg.ESDCOR0026.f") (runAction(getObject("form").value,"E...	400
53	Save	Save	getObject("last_used_action_id").value=""; clearNonSystemRequired(); save...	300
56	Apply Ticket Template	Apply Ticket Template	if(getMenuGroupObject("ApplyTicketTemplate").isLoading & getMenuGroupO...	700
122	Close	Close	topx.close(); return;	600

Record(s) 1 to 20 of 24

Toolbar #103 : Print

Related To Form: Configuration Item Toolbar Name: Print Toolbar Item: Print Sort Order: 450

General Information

Toolbar Code

```

if(hasChanged) { if(confirm("$(@msg.ESDCOM0015.f") { if(save()) { return; } } else { return; } }
openFormEx("ESD_RPT005_FROM_CI_PREVIEW&ci_id=" + getObject("row_id").value + null, 1020, 685, 0,
0, "false", "location=0,menubar=0,status=1,toolbar=0,scrollbars=auto,resizable=1","auto", false); getMenuGroupObject("print").style.visibility
="hidden"; return;

```

A list of items on the toolbar is available in the table. You can filter the list to view the items depending on the form type.

To view and modify details on an item listed, you can click on an item in the list. Details will be displayed in the form below. The form area contains the toolbar description, which is a code for the Toolbar item. It also contains the Permissions Tab.

Managing Toolbar Options allows you to limit the actions that the Service Desk Agent can take on the form. Take the instance of a Level 1 Service Support Group - this group is responsible only for receiving the request, creating the ticket, and forwarding the request to another group.

The Level 1 support Group would be able to use Toolbar Items like Create New and Copy to new Options. However, this group would not find options of Add to Knowledge Base and Print useful.

Or, you would not want to allow the group to print the ticket or Add solutions to Knowledgebase. You can therefore not grant permissions for these options from the ticket tab.

The Level 2 Service Support Group would actually works on the ticket towards resolving the issue and closing the ticket and you would provide access and permission to the group accordingly.

The support group, and contacts related to that group see only those options on the Ticket Toolbar that they have been granted permission to view. Thus, you can control what the support group does with the ticket and provide an uncluttered toolbar for a specific support group.

Ticket Custom Fields

All Ticket forms have a fixed set of Attributes that allow you to capture standard information for a ticket. This includes fields for capturing Requester Information, Ticket details like description, Categorization, Priority, urgency, Severity, impact, etc., depending on the type of ticket. However, there could be additional details that are not captured in the standard fields.

To capture such additional details in a systematic and standardized way; you can configure Custom Fields on tickets. The Custom Fields can be grouped into sections by providing a Section Header; and by specifying an Order for the field, you can place the field appropriately on the Tickets.

Manage Attributes

The Manage Attributes link under Application Set up allows you to create a pool of attributes that can be used to create Custom Fields for tickets and configuration items. The Attributes List table lists all available Attributes .

You can view an existing attribute, and modify its Values as appropriate. You can also create new attributes.

To create a new attribute, you have to specify Attribute Name (a Required field), Attribute Type, Attribute Unit, Sort Order , and possible values. You will not be able to delete an attribute that is already used on any Custom Fields for tickets or for Configuration Items .

The screenshot shows a web form titled 'Attribute Name # 76 : CD Drive'. At the top right are buttons for 'Apply Changes', 'Create New', and 'Delete'. The form contains the following fields:

- Attribute Name:** A text input field containing 'CD Drive'.
- Unit:** An empty text input field.
- Sort Order:** A dropdown menu currently showing '0'.
- Attribute Type:** A dropdown menu that is open, showing a list of options: Text, Number, DateTime, List, MultiLineText, Checkboxes, Radio Buttons, and Section Header. 'Section Header' is highlighted with a blue background.
- Possible Values:** An empty text area for listing possible values.

The same attribute can be used on multiple Ticket Templates. The possible value options control the Value a user may insert in the form where the attribute is used. The Manage Attribute type dropdown contains an option 'Section Header'.

This allows you to create a pool of Section Headers that can be used on different ticket forms.

To configure a Section Header; you can type in an Attribute Name as appropriate; and select Type as Section Header.

When configuring a Custom Field template, you can pull out the section header and use it on the template. All other attributes that are to be grouped under the header can then be grouped as appropriate.

Note: In Nimsoft Service Desk, combinations of Double Tilds (~) and Double Pipes (||) is used with specific purposes.

Therefore, these combinations must not be used in any input fields in the application. This can cause the system behavior errors that can be corrected only with engineering intervention.

Manage Custom Fields Templates

The Manage Custom Fields link under Application Setup allows you to configure Custom Fields on tickets. Clicking on this link displays a list of available Custom Field Templates. You can click on an item in the list above to view details of the template.

Create New:

You can create new Custom Field templates using the form below. To create a new template, a required field is Related to form. You can relate a custom field template to any one Ticket form and specify a name for the template. Once you create and save the template, you can add Attribute to the form.

The screenshot displays the 'Application Setup (Manage Custom Field Templates)' interface. It includes a 'List Filters' section with a search bar and a 'Custom Field List' table. Below the list is a 'Custom Field Details' section for the selected template 'My Test'.

Custom Field List:

ID	Form Name	Template Name	Description	Status	Modified Date
25	Service Request	Linksys Wireless Routers	Linksys Wireless Routers	Active	16/07/2010 11:43:45 AM
26	Task Ticket	My Test	My Test	Active	08/03/2011 07:58:08 PM

Record(s) 1 to 2 of 2

Custom Field Details:

Custom Fields Template #26: My Test

Related To Form: Task Ticket, Template Name: My Test

Description: My Test, Status: Active

Created On: 08/03/2011 07:57:55 PM, Created By: Demo, Admin

Modified On: 08/03/2011 07:58:08 PM, Modified By: Demo, Admin

Attributes: Related CCT

Section Header	Attribute Name	Attribute Default Value	Unit	Sort Order	Required On Submit?	Visible To SSU	Status
	Cache	1	KB	0	No	No	Active

Record(s) 1 to 1 of 1

Add Attributes:

To add an attribute, you have to choose an attribute from the Attributes Pool (using the lookup). The attribute type and possible values get automatically updated when the attribute is selected. To specify where the attribute appears of the ticket form, you can specify an order for the Attribute.

You can also choose whether the field is to be a Required field and whether the field will be Available to Self-Service Users or not.

Section Header:

You can group the Attributes into sections by choosing a Section Header from the Attributes Pool. All attributes related to that section will be clubbed under the section header in the order specified.

Relate CCTI:

You can relate Custom Fields Template to multiple CCTI of tickets. When a ticket, with any related CCTI is logged; the Custom Field Template automatically gets associated with the new ticket. When the ticket is saved, the custom fields become available in the Additional Information Tab of the ticket.

Modify Existing Custom Field Template:

You can also modify existing custom field templates. You can add new Attributes to an existing custom field template, regroup existing attributes by changing the section headers, or change the Sort Order of the attribute. You can also relate or unrelate the template to a CCTI from the CCTI tab.

The changes take effect immediately; and become available on new ticket forms where they get applied.

However, the changes will not impact older existing ticket records where the template is used. You can manage the Status of an attribute used in a custom template as active or

inactive and also define the status of the Custom Field Template as Active or Inactive .

If custom fields have been included in a Ticket Template made available to the Self-Service User, the ticket form will contain a section called Additional Information. This section contains all the Custom Fields that are applicable to that ticket.

Service Desk Agents can see Custom Fields on tickets in the Additional Information Tab of the ticket. In this tab they will see the custom fields that are applied to the ticket based on ticket type and CCTI. The custom fields will be grouped into sections with a Section Header, if so configured.

Custom Fields can be used for configuring Auto-Routes, Workflow Actions, Defined Searches, etc. These fields can also be used for Advanced Search, when printing a ticket, and when extracting reports on tickets.

Administering Ticket Functionality

Besides configuring Workflows for tickets and setting up Workflow Action for tickets, you will be taking up some initial setup activity to configure the ticket functionality as per your Organization needs.

This section identifies the activities that you will undertake to manage the ticket and Ticket related functionality for Service Desk Agents and for Self-Service Users.

Work and Time Tracking

All ticket forms have a Worklog section where Service Desk Agents can enter details of work done towards a ticket that they are working on. They can classify the worklog based on Worklog Type and choose to make the Worklog visible to the customer by choosing either Yes or No in the Client Viewable field.

Agents can also indicate the time spent towards an activity that is being reported in the Worklog . The total time spent field displays the cumulative time spent on a ticket. This can be used to calculate effort put in towards issue Resolution or closure.

Mark as Required Fields:

As Application Administrator, you can Set Fields related to the worklog section as Required Fields . You can make time tracking as a required field on all tickets by setting the value of the Configuration Parameters REQUIRE_TIME_TRACKING_ON_ALL_TICKETS as Yes.

You can also make Worklog Description as a Required Field in workflow actions. This helps ensure that worklog related information is captured on tickets.

Self-Service Users can also add a Worklog update to their tickets if they want to update information related to their ticket. The stakeholders of the ticket get notified about this update and the update is visible on the Activity Tab of the ticket as Client Note .

Send as Mail:

Service Desk Agents working on tickets can send their Worklog as email to intended recipients. To enable this feature, you have to set the Configuration Parameters ALLOW_EMAIL_DELIVERY_ON_WORKLOG_ENTRY as Yes.

If this feature is enabled, a Send as Mail checkbox is displayed in the worklog section. To use this feature, Service Desk Agents can check this checkbox before they save the worklog. Upon saving the worklog, a communication template opens. The body of the email contains the updated worklog.

The agents can choose recipients and send the Worklog as email to the selected recipients.

Activity Tracking

The Activity Tab on the ticket displays entries related to all the actions taken on the ticket, and all communications sent out and received by the ticket.

Actions on the ticket include manual and automatic actions executed on the ticket, leading to change in status and reason code, and all worklog entries added to the ticket by the Agent/Analyst working on the ticket.

Communications listed in the Activity Tab include all notification related communications that gets sent out as per the workflow or auto-routes that get applied to the ticket; and other communication generated such as SLA target related notifications etc.

You can click on an item listed in the table to view all details of the action or communication.

The communication details page displays all details like communication type (Phone/Email), communication status, and details of the actual communication sent out.

If a communication was made by phone in response to an SLA Phone* notification, the Notification ID field will contain the unique ID associated with each communication sent out by MIR3 notification system. This ID can be used to check details of the communication from the MIR 3 site.

Note: For enabling SLA Phone Notifications, you will need to buy a license from MIR3. Phone Notification is an external service provided by MIR3, and not a default feature available with Nimsoft Service Desk.

Currently Phone Notifications are supported only for SLA Notifications, and not other notifications sent out by the application

SLA Compliance Monitoring

Nimsoft Service Desk allows you to configure SLA monitoring for tickets. As application administrator, you can determine whether you want to initiate SLA monitoring or not. You can enable SLA monitoring by setting the Config Parameter `ENABLE_SLA_MONITORING_ON_TICKETS` as Yes.

If this parameter is set to yes, all tickets will display the SLA Compliance tab. This tab will display any Service Target that gets applied to the ticket, when the target got applied to the ticket, status of the target – like Missed SLA, Met SLA, Approaching Violation etc.

Agents can use this information to plan and prioritize their ticket queues. You can generate reports related to SLA compliance to monitor compliance and set service standards.

Configuring Service Level Management is dealt with in detail in the related system.

Defined Searches

Often, users tend to search for specific type of information frequently. Therefore, Nimsoft Service Desk allows the Users to sift through tickets and other records to search for a specific record or for records matching certain conditions.

For example, Service Desk Agents may want to see Open Tickets for their Support Group(s), or search for Configuration Items that are related to them.

For such frequently used searches, you can configure a Pre-defined Search query and make that query available to Service Desk Agents; or different Support Groups based on the activities they undertake and their search needs.

Nimsoft Service Desk provides a pre-configured set of Defined Searches for most frequently searches. As administrator, you have default access to all Defined Search queries. You can manage Permissions to existing defined searches and configure new defined searches as per your organization needs.

Service Desk Agents (and Administrators) can access the defined searches from the Search link under each ticket module and for Configuration Items.

As application administrator, you can enable or disable access to the pre-defined searches from the Manage Defined Searches link under Workflow Tools. Clicking on this link displays a list of available Defined Searches.

The screenshot displays the 'Workflow Tools (Manage Defined Searches)' interface. On the left, there are three red boxes with labels: 'Filter List', 'Defined Search List', and 'Defined Search Details'. The main area shows a table of defined searches with columns: ID, Related To Form, Category Name, Search Name, Help Text, and Sort Order. Below the table, the details for 'Defined Search #29: All Scheduled Approved Change Req...' are shown. This includes fields for 'Related To Form' (Home, Change Request), 'Search Name' (All Scheduled Approved Change Requests), 'Category Name' (Default), and 'Help Text' (All scheduled change requests that have been approved and awaiting implementation). The 'Query' tab is selected, showing a complex SQL query. The 'Permissions' tab is also visible.

ID	Related To Form	Category Name	Search Name	Help Text	Sort Order
2	Home, Service Request	Default	My Group's Open Service R...	My Group's Open Service Requests	2
3	Home, Service Request	Default	Tickets Not Assigned to Any...	Tickets Not Assigned to Any Group or Individual	3
4	Home, Service Request	Default	Service Request Updated w...	Service Request Updated within last 7 Days	4
5	Home, Service Request	Default	Open Service Request Not U...	Open Service Request Not Updated within La...	5
6	Home, Service Request	Default	Open Service Request Appr...	Open Service Request Approaching SLA Viol...	6
7	Home, Service Request	Default	Open Service Request Violat...	Open Service Request Violating SLAs	7

Defined Search #29: All Scheduled Approved Change Req...

Related To Form: Home, Change Request

Search Name: All Scheduled Approved Change Requests

Category Name: Default

Help Text: All scheduled change requests that have been approved and awaiting implementation.

Query: `CAST(case_id AS VARCHAR) = CAST(ticket_id AS VARCHAR) AS Case#, ticket_type AS 'Ticket Type', created_date AS 'Created Date', ticket_status AS Status, ticket_description AS 'Symptom Description', ticket_resolution AS 'Resolution Order' (formatted to last name * * * * * assigned to name) AS 'Assigned To'`

Search Condition: `APPROVAL_STATUS = 'Approved'`

You can view details of a particular search by clicking on a specific item in the table. The details will be populated in the form below. You can view the search query in the details section. You can manage access to the defined search for specific Support Groups or Roles from the Permissions tab.

You can also configure a new Defined Search by configuring a query by defining the Matching Conditions. The Preview results action allows you to view the results of the data displayed. You can enable or disable access to a defined search from the permissions tab.

Reports

Nimsoft Service Desk stores historical data of all transactions related to tickets. This historical data can be used to generate a variety of reports related to tickets and ticket related entities. A range of pre-configured reports related to Ticket trends, SLA Compliance trends, Configuration Items, etc. can be seen as On Screen reports or be generated as PDF or CSV files.

You can enable or disable permissions for Service Desk Agents to access the reports. You can enable or disable permissions to the Reports link under the Ticket Modules by disabling permissions from the Manage Navigation Menu action. You can also control which reports are accessible to specific Support Groups , Roles, or contacts by enabling or disabling permissions to a specific report.

You can manage reports from the Manage Report Configurations link under Admin Utilities. Clicking on this link displays a list of available reports. To view details of an available report, click on an item in the table. The details will get populated in the form below. You can manage permissions to access and view a specific report from the Permissions Tab.

Service Desk Agents have access to a Reports Link under all ticket modules as well as in Management and Knowledge Management section. As application administrator, if you want to permit Service Desk Agents to view reports, you have to enable access to the Reports link and to the individual reports that the Agents will be permitted to access.

All available reports can also be accessed in the Trends and Metrics Module in the Navigation Menu. The reports are grouped under different heads in this section. You can enable or disable permission for access to this module for Service Desk Agents.

Dashboards

Users of Nimsoft Service Desk can access a range of dashboards to view trends related to Tickets and Configuration Items. Besides the Dashboard Charts that are displayed in the Home Page and the List Tickets page of each ticket module, Service Desk Agents and Administrators can also view other dashboards in the My Dashboard Link under Home.

As Application Administrator you can enable or disable permissions for a specific Support Group or Role to access the My Dashboard link. You can also control their ability to view and access specific Dashboard Charts.

You can manage Dashboards from the Dashboards Link under Application Setup. Clicking on this link displays a list of available Dashboard Charts. When you click on a

specific item in the list, the dashboard gets displayed in the details tab. Users can modify some aspects of the Dashboard; like change the Grid layout, increase or decrease the image size etc.

As application administrator, you can also create new Dashboards and make these Dashboards available to different Support Groups and roles. One main Pre-requisite to configure a new dashboard is configuring charts that are displayed in the Dashboard. Charts are drawn from pre-defined search queries associated with the chart. This is dealt with in detail in the Advanced Configurations section.

Ticket related Config Parameters

You can enable or disable a functionality related to tickets or set default setting related to specific ticket functionality as per the needs of your IT support by setting appropriate values in the associated Configuration Parameters .

- Configuration Parameter related to Request Management help you define functioning of the Service Requests
- Configuration Parameter related to Incident Management help you define functioning of the Incident tickets
- Configuration Parameter related to Problem Management help you define functioning of the Problem tickets
- Configuration Parameter related to Change Management help you define functioning of the Change tickets
- Configuration Parameter related to Task Management help you define functioning of the Task tickets
- Configuration Parameter related to System help you define functioning common for all ticket modules and generic functionality such as enabling or disabling Case ID, Ticket Phase, worklog related Required Fields etc
- Configuration Parameter related to Self-Service help you define functionality for Self-Service Users

How Do I

Below are some actions you can take related to Ticket Functionality.

Modify values on ticket fields

You can modify values of attributes that appear on standard ticket fields and rename them as per the field naming conventions followed in your organization. The field values that you can modify are Impact, Priority, Source, Urgency and Worklog Type.

To modify values on ticket fields:

Step 1: Click on Manage Value List link under Workflow Tools. A list of values per ticket type is listed in this form.

Step 2: Click on the Value List item (Impact, Priority etc.) that you wish to modify.

The details of the value like Display Value, Sort Order and Background color will be displayed. You will also see an option of Set as Inactive.

Step 3: Click on the Display Value of the Value you wish to modify.

You can rename a Value as per your naming convention (For example, you can change the default values of Impact from None, High, Medium, Low to Minor, Major and Severe).

You can also set a display value as Inactive, or delete a display value option.

You can set column highlighting based on field values. The color which gets applied to show highlighting can be selected in the Background Highlighting field.

Step 4: Click on Apply Change to save the modifications made.

The modifications will get applied on the tickets immediately. However, older records where the value was used will not get impacted. The modified values will be available on open ticket and new tickets created thereafter.

The Display Value Options could be used in Set Fields on Action Options or a Matching Conditions for Auto-Routes, Action Options or Approval Groups. Modifying Values after configuring other entities and records could lead to some disruption in how these records function or get applied.

The Display Value Options for Home (Status related options) are Hard Coded and cannot be modified. You can only make cosmetic changes to these like apply highlighting or modify Sort Order.

Control items available on the ticket toolbar

You can control the items available on a Ticket Toolbar, Configuration Item Toolbar, and Knowledge Article Toolbar by enabling or disabling permissions to the item.

To control availability of an item in the toolbar:

Step 1: Click on the Manage Toolbar Menu link under Administration Utilities. A list of all Toolbar Items will be listed in the form.

Step 2: Click on the Toolbar Item that you wish to manage access to.

The Toolbar Item details will be displayed in the form below.

Step 3: Click on the Permissions Tab to view details on permissions currently enabled for.

To provide or revoke permissions, click on the Manage Permissions action button. The Permissions lookup will be displayed.

Step 4: Select contacts, users, or roles to whom you wish to enable permissions in the Select Permissions to be Granted section.

You can revoke permission by selecting the user, support group, or roles and clicking on Remove.

By enabling or revoking permission to an item on the toolbar, you can control the actions that Support Technicians or Agents take on a ticket, configuration item or Knowledge article.

You can also configure a new Toolbar Item. However, the Toolbar Code that you configure has to be logical to render the toolbar item in the menu.

Create Custom Fields on tickets

You can create Custom Fields on tickets from the Manage Custom Fields link under Application Setup. To view and modify existing Custom Fields and to create new Custom Fields:

Step 1: Click on the Manage Custom Fields link under Application Setup. The Manage Custom Field Templates form will display a list of all active Custom Field Templates.

You can modify existing Custom Field Templates and create new Custom Fields Templates in the form below. To create new Custom Fields Template:

Step 2: Select the Ticket Type the Custom Field Template is to be related to. You can relate a Custom Field Template to only one ticket type from Service, Incident, Problem, Change or Task Ticket.

Step 3: Enter a Name for the Custom Field Template in the Name field, which is a required field.

You can add a description to provide more information. However, it is not mandatory, so you can choose to leave this field blank.

Step 4: Click on Apply Changes to save the Custom Fields Template record.

When you save the record, the Attributes section will get activated and you will be able to add attributes to the template. The Related CCTI tab also gets displayed on the form.

Step 5: To Add Attributes to the Custom Field Template, select an Attribute in the Attribute Name field. The Lookup will display a list of all Attributes in the Attribute Pool.

When you select the Attribute, related aspects like Attribute Type and Units will get updated automatically, based on the values configured for the Attribute.

Step 6: You can choose to group the Attributes in sections. To group the Attributes, choose a Section Header from the Attribute Name Lookup. This lookup will display only those Attributes that have been marked as Section Headers.

Step 7: Assign a Sort Order to the Attribute. This will control the position at which the Attribute will appear within the template.

Step 8: If you want to make the Attribute available to Self-Service Users when they log a ticket from the Self-Service User interface, you can check the Visible to Self-Service User checkbox.

Step 9: If you want to mark the Attribute as a Required Field, you can check the Value Required on Submit Checkbox.

Step 10: Click on Save Attribute to add the Attribute to the template.

You can repeat Steps 5 - 10 for each Attribute you wish to add to the Custom Field Template.

Once you have finished adding Attributes to the Custom Fields Template, you can relate the template to CCTI that the template applies to.

Step 11: Click on the Related CCTI Tab to relate the template to available categorization.

Step 12: Choose the Class of the CCTI you wish to relate the Custom Fields Template to. You can also choose Class, Category, Type and Item if appropriate.

The Custom Field Template will get related to all tickets of a specific type with have the related CCTI. All custom fields will appear in the Additional Information Tab of the tickets where the template gets applied.

Note:

Attributes have to be configured before configuring the Custom Fields Template (Manage Attributes)

Attributes called Section Headers have to be configured for grouping Custom Fields into sections.

The Custom Field Template will not get related to any ticket if Related to CCTI is not specified.

Grouping of custom fields into sections using a Section Header is controlled by Slice Configuration. To allow grouping of custom fields, the parameter value of the configuration `ENABLE_GROUPING_OF_CUSTOM_FIELD_INTO_SECTIONS` has to be set to yes.

Frequently Asked Questions

You can find answers to some common questions you may have related to managing value lists and managing custom fields on tickets.

Manage Value List

What does the sort order of a Value (for any item) indicate?

The Sort Order of a Value indicates the order in which the value option appears in the drop down list. For example, if Value Options for Priority are Critical, Urgent, High, Medium and Low, the items will appear in the Sort Order specified (the lowest sort order appears first).

What happens if I set a value as Inactive?

If you set a value option as inactive, the inactive value option will not be displayed in the respective dropdown list for the field. This means that the Service Desk Agents (or anyone working on the ticket), will not be able to view the inactive value in the respective dropdown list and set the field value accordingly.

However, setting a field value option will impact auto-routes or action options where the value option is set as a matching condition because the value option will not be available for use as a matching condition. Also, if the inactive value is identified as a Set Field value, the system will not be able to execute the set field value action.

If I make a value active again, will it be visible on older records as well?

Yes, if you make an inactive value as active again, it will be available for use of existing open tickets as well. The value option will appear in the related dropdown list for existing as well as new tickets.

The value will also be available for auto-routes, action options, and other defined actions.

Can I modify value for all tickets at a time?

No; you have to set value options for one ticket at a time. No bulk action is possible as only one record can be modified at a time.

Manage Custom Fields

Can I relate a Custom Field Template to multiple forms?

No. A Custom Field Template can be related to only one form type. The dropdown list does not allow you to select more than one form.

Do I have to relate a Custom Field Template to a CCTI? What happens if I do not associate the template to any CCTI?

Yes, you have to relate a Custom Field template to at least one CCTI for tickets. A Custom Fields Template gets applied to tickets based on the ticket CCTI. There fore, if a template is not related to any CCTI, it shall not be applied to any ticket.

What happens if I add a new attribute to a Custom Field Template - will it be automatically available for older ticket templates?

The new custom field will not be available on older tickets. The ticket record will continue to display only the fields that get applied to it during the ticket initial creation (when the ticket was first saved).

However, going forward, when the custom field template is invoked on a ticket, the new field will be available as configured.

Will new Custom Fields on a ticket change if the CCTI of the ticket is changed?

No; once the ticket is created and first saved, Custom Field template related to the Ticket CCTI gets applied to the ticket. Subsequent modification of the CCTI does not lead to older fields getting removed or newer fields getting added to the ticket.

Will Self Service Users be able to view and use all Attributes on a Custom Field Template?

Yes; when configuring Custom Field Templates, you can enable or disable ability for Self-Service Users to view and add input into custom fields. By checking or unchecking this field, you can control the ability of Self-Service Users to see a custom field.

Can I make only few Custom Fields available to Service Desk Agents?

No; Service Desk Agents will be able to view all Custom Fields in a Custom Field Template when the template gets applied to a ticket. This is because the Service Desk Agents work on the ticket. Custom Fields are configured for tickets so as to aid Service Desk Agents in seeking and adding information critical to working on the ticket. Hence, hiding some fields from the Agents serves very little value.

Can I make a specific attribute a Required Field to ensure that the field is filled in before submission?

Yes; when creating a new attribute or custom field, you can specify it as a Required Field. If so specified, you will be able to ensure that the user puts in appropriate values in the field.

What happens if I delete an Attribute from a Custom Field template? Will it impact older records?

Deleting an attribute from a custom field template does not impact older records. Going forward, when the custom field template is invoked, the Attribute will not be available.

What happens if I delete/deactivate a Custom Field Template? How does it impact older records?

Making a Custom Field template inactive does not impact older records. The template will not be available for future use.

Can I use Attributes on Custom Field Templates when configuring Auto-Routes or workflow actions?

Yes, custom fields can be used when configuring Auto-routes and workflow actions. The Matching Conditions section of the Action Option or Auto-Route record has fields

labeled Attributes (1-6). You can use these fields to set Custom Fields as Matching Conditions for tickets.

Chapter 21 - Manage Ticket Templates

Overview

Templates can be used to provide a structured format for seeking information to log a request, or providing specific information about the request. Templates can be configured to have substantial data and structure and yet remain flexible to be modified as per need of the specific transaction.

Configuring templates enables re-usability, reduces effort of the end-users, and brings in standardization in terms of structure and format. Templates can be configured for submitting standard requests (Ticket Templates) and for managing communication about a transaction related to a ticket (Communication Template).

Configuring Ticket Templates ensures that all information essential for working on and resolving a request is available. Configuring communication template enables automating notification on a ticket transaction and also ensures standardization of the Notifications sent manually by different users.

Access to all templates is managed by Permissions. As administrator, you can access available system-defined Communication Templates, and configure new Communication Templates to suit your requirement and assign permission for contacts, support groups, and roles to access these templates.

A Request Catalog, comprising all accessible Ticket Templates can be accessed by Self-Service Users from the Self-Service User Interface. A ticket logged by the Self-Service User using a template from the Request Catalog can get auto-routed to a specific support group rather than to the default assignment group.

Service Desk Agents can access Ticket Template for a specific Ticket type from within each Ticket Module. The Create ticket (using template) link displays a list of all template for that ticket type, which they have permission to use. This section explains the process of setting up Communication Templates, Ticket Templates, Task Groups, and Task Flows.

Create Ticket Template

In the context of IT support, there are requests that can be predicted; and that are often requested for by the users. This could include request for permissions to use or access an IT resource, reporting unavailability of an IT object or Service, or request for some standard modifications like upgrade to a latest version of a software.

For such frequently requested tickets, you can configure Ticket Templates. The templates can be pre-populated with baseline information and contains place-holders for additionally needed information. This makes the process of logging a request faster, easier and more standardized.

You can set Values for the standard ticket fields and Custom Fields on the ticket form. These are displayed as pre-filled fields when the template is used. You can set specific 'Assigned to Group' for a template and override any existing Auto-Route that could get applied to the ticket.

Create or Modify Template

You can manage Ticket Templates from the Manage Ticket Template link under Workflow Tools in the Navigation Menu. Clicking on this link displays a list of available templates. You can filter the list from the available filter options.

To view any item in the list, click on the item in the table. Details of the existing template get populated in the form below.

You can modify existing templates by adding or removing Set Fields on the template or change the status of a ticket template (Active or inactive). You can also create a new Ticket Template using the Manage Ticket Template form.

Workflow Tools (Manage Ticket Templates)

Filter By: Ticket Type | Category | Search

ID	Ticket Type	Category	Name	Description
2	Service Request	New Employee	Create NT and E Mail	Create NT and E-mail Accounts
3	Service Request	General	Create NT and Server Account	Create Network and Server Accounts
4	Change Request	General	Standard CR_Build and Deploy PC N...	Build and Deploy Desk Top for New User(CHG)
5	Change Request	General	Standard CR_Create NT and E mail ...	Create NT and E Mail Account
6	Task Ticket	General	Create NT and E Mail Account	Create Network and E Mail Account
7	Service Request	General	Configure LAN drop for VLAN-1	Configure LAN drop for VLAN
8	Task Ticket	General	Configure LAN drop for VLAN	Configure LAN drop for VLAN
9	Task Ticket	Telecom	Set Up Telephone and Voice Mail	Set Up Telephone and Voice Mail
11	Task Ticket	General	Create Home Directory	Create Home Directory

Record(s) 1 to 20 of 47

Ticket Template #7: Configure LAN drop for VLAN-1

Ticket Type: Service Request Category: General Name: Configure LAN drop for VLAN-1 Override Auto Routing: ☐

Description: Configure LAN drop for VLAN Auto Assign Action: ☐ Auto Assign On Create: ☐

Set Fields

Field to set	Value
Remove: (ccfi_id)	Select HR
Remove: Reason Code (ticket_reason_code)	None
Add: (affected_ci_id)	To add another field, select it from the drop-down menu and click on Add.

The main fields in the ticket template form are listed below.

Field Name	Detailed Description
Ticket Type	This field lets you choose the ticket type which the template is related to.

Category	You can classify a template by assigning Category. The template will be grouped by the category name in the Self-Service User Interface.
Name	You have to assign a Name to the template as the template Identifier. This is a required field.
Description	This field is used to provide a brief description about the template, its purpose etc.
Override Auto-Routing	You can manage assignment of the ticket by overriding any Auto-Route that may get applied based on the ticket Matching Conditions.
Auto-Assign Action	This action is available only on Task Templates. You can choose from the available auto-assign actions in the lookup.
Auto-Assign on Create	This action is available only on Task Templates. The ticket gets auto-assigned without manual intervention.
Set Fields	This tab lets you choose the fields on the template to be pre-populated. You can choose a field and pre-fill appropriate Values in the field.
Permissions	This tab lets you manage permissions for access to the template.

The Set Fields tab on the ticket template allows you to select fields on a ticket form; and pre-populate it with relevant information. You can choose to set either standard ticket fields; or custom fields on the ticket.

You can choose a relevant field on the ticket from the dropdown list in the set field tab. All fields on a ticket are listed in the dropdown. The standard fields on the ticket are listed at the top; followed by a listing of the Custom Fields.

A ticket template can be related to only one ticket type. You can set all appropriate fields on the ticket form; this includes the standard ticket fields as well as the custom fields on the ticket. Permissions for the ticket template can be assigned to contacts, Support Groups and roles.

You can modify an existing ticket template; and the changes become applicable on all new transactions using the template. Older records, however, remain unchanged. You can manage Status of a ticket template and make the template Active or inactive. Users can access only Active templates for their transactions.

Set Fields on Ticket Template

The Set Fields tab on the ticket template allows you to select fields on a ticket form; and pre-populate it with relevant information. You can choose to set either standard ticket fields; or custom fields on the ticket.

You can choose a relevant field on the ticket from the dropdown list in the set field tab. All fields on a ticket are listed in the dropdown. The standard fields on the ticket are listed at the top; followed by a listing of the Custom Fields.

You can choose appropriate standard fields like Status, Reason Code, Phase, Impact, Priority, Urgency, Description, CCTI, etc and Set values for these fields. You can also choose all appropriate custom fields where setting field value will assist in the ticket processing.

When users access the ticket; the set field values will be automatically populated. They can modify these values as appropriate. If custom fields are set; the Additional Information section/tab of the ticket will display the set field values for Custom Fields.

Notes:

Not all fields listed in the dropdown are relevant or useful for configuring a ticket template. You must therefore; exercise discretion and care while setting fields on Ticket Templates.

- Case ID and Ticket Id fields should not set, because they are auto generated.
- For fields such as Status or Reason Code, if included in the Set Fields, a value must be specified.
- For Assigned Group Id or Assigned Individual Id, if included in the set field, Values must be specified

- If specifying value for fields like class, category etc. manually; matching value must exist in the CCTI records.

Task Ticket Template

Task tickets are created as Child Tickets for Incident, Problem, Change or Service Requests. When configuring template for Task Tickets; option of Auto-Assign Action and Auto-Assign on create are enabled. This allows you to manage action on task ticket and assignment of task ticket created using the template.

When configuring a Task Ticket Template; you have to set field values for Task Name and Task Description as these are Required Fields on a task ticket. All other field Values can be set as per your needs.

These options are available only when the slice Configuration Parameter `Enable_Auto_Routing_of_Task_Templates` is set to Yes. The auto-assign action allows you choose from available actions in the lookup. You can also choose to auto-assign task when it is created. This enables automatic assignment of the task ticket to the specified assigned to Individual or Group.

If auto-assign action is configured; but auto-assign on create is not checked; the system will look for assigned to details in the set fields. If no details are found; the ticket will get automatically assigned to the contact who has created the task ticket (the logged in user); who can then assign the ticket to the specified contact or support group as appropriate.

Manage Permissions

A Ticket Template can be related to only one ticket type. The template will be available in the Template list of the related Ticket Module (log ticket using template link) for Service Desk Agents. This link will display a list of all templates that have been granted permissions for. Service Desk Agents can also access all available templates under Create Ticket (Using Template) link under Home.

Self-Service Users can view a list of all templates available to them in the Request Catalog link under Issue Services in Self-Service User interface. If a Category Name is specified for a template; and permission to the template is enabled for Self-Service Users; the Ticket Template will be displayed under the category name in the Request Catalog. If no category is specified; the template appears under General Category.

Manage Ticket Template Check Points

Some key elements to keep in mind when configuring Ticket Templates are:

- A Ticket Template can be related to only One ticket type.
- Access to the ticket template is controlled by Permissions

- You can control an Auto-Route getting applied by checking on Override Auto Routing checkbox.
- Auto-assign action and auto-assign on create are available only for task tickets
- Auto-assign action is controlled by a slice parameter
- As not all fields listed in the set field name dropdown list are meaningful; caution is needed when selecting a field.
- Appropriate value has to be filled in while configuring a template; for the template to be meaningful and usable.

How Do I

Below are some actions you can take related to Ticket Templates.

Configure Ticket Template

You can configure Ticket Templates from the Manage Ticket Templates link under Workflow Tools section in the Navigation Menu. To configure a Ticket Template:

Step 1: Click on the Manage Ticket Templates link. A list of active Ticket Templates will be displayed in the list.

You can modify an existing Ticket Template or configure a new Ticket Template in the form below. The steps to create a new Ticket Template are listed below.

Step 2: In the Ticket Type field, select the form the Ticket Template will be related to. You can choose any one Ticket Type from the dropdown list.

Step 3: Create or choose a Category for the Ticket Template. You can choose a category from the lookup, or create a new Category. The newly created category will get added to the list and will be available for choosing for other ticket templates.

If you don't choose a category, by default 'General' category will get selected.

Step 4: Enter a Name for the Ticket Template in the Name field, which is a required field.

You can provide additional information about the Ticket Template in the description field. However, this is not a required field. You may leave it blank.

Step 5: To control application of an auto-route to ticket created using the template, you can check the Override Auto-Route checkbox.

The fields of Auto-Assign Action and Auto-Assign on Create are specific to Task Templates. They will be enabled only when the Ticket Type selected is Task.

Step 6: Click on Apply Changes to save the Ticket Template.

Once the Ticket Template is saved, further configuration features will get displayed on the form. The Set-Fields Tab will display the Field to Set and Value table. The Permissions Tab will appear on the form.

Values entered in the Set Fields section get displayed on the ticket when the Ticket Template is used to log a request. Values in fields like Assigned To Individual or Assigned to Group help in routing of the ticket.

To Set Fields on the Ticket Template:

Step 7: Select the Ticket Field that you want to pre-populate. You can choose from Standard ticket fields as well as Custom Fields on a ticket to set fields. Select a field in the dropdown list and click on Add. The Field will get selected.

Once you add the field, the value column will display a select option, a dropdown list, or a free text field, depending on the value type accepted by the field.

Step 8: Set a Value for the Field. Depending on the field type, you can select a value from the dropdown list, choose from a lookup, or enter appropriate free text.

If the field value allows you to select from a lookup, for example, Assigned to Group or CCTI ID, the value column will display a Select Button. You can click on this button and choose a value from the lookup that gets displayed.

You can choose as many fields as you wish to set on the ticket. Once a field is set, a 'Remove' action button will be displayed. You can use this to remove set fields.

Step 9: Click on Apply Change to save the Set Field Values you are setting.

Step 10: Enable permissions for access to the Ticket Template. By default permission is enabled only for Administration Group. You can grant permissions to selected users, support groups or roles.

Note:

You must exercise care in selecting fields where adding Set Field values assists in ticket logging, routing and processing.

When setting field values for CCTI, it is advisable to select CCTI ID, rather than individually select from Class, Category, Type and Item. Choosing CCTI ID will display a select lookup from which you can select appropriate options. If you select individually, you will have to type in corresponding values.

Case ID details are auto-generated. You cannot set field values for these fields.

Configure Task Ticket Template

You can configure Task Ticket Templates in the same way as you configure other Ticket Templates. (Refer to How Do I Configure Ticket Template for detailed steps). Additional configurations applicable for Task Ticket Templates are discussed below.

To Configure Task Template:

Step 1: Click on Manage Ticket Template link to access Ticket Template form.

Step 2: In the Ticket Type field, choose Task Ticket from the dropdown list.

Step 3: Choose Template Category, Template Name and Template Description as appropriate.

You can choose Override Auto-Routes if you want to keep the ticket out of the auto-routing process.

Step 4: You can choose a workflow Action that gets applied to the Task Ticket Template from the Auto-Assign Action field. Click on the lookup to view Action Options applicable to Task Tickets.

You can choose what action gets executed when the Task Ticket is created using this Task Template.

Step 5: If the action you have chosen is related to Assignment (Assign to Individual or Assign to Group), you can check the Auto-Assign on create checkbox.

If this checkbox is checked, when the Ticket Template is used to create a Task Ticket, the ticket gets automatically assigned to the Assigned to Individual or Group specified.

Step 6: Set Fields for the Task Template by selecting the fields to be set and corresponding field values.

Step 7: From the Permissions tab, assign Permissions for access to the Task Template to users, support groups and roles.

The added features of Auto-Assign Action and Auto-Assign on Create are applicable only to Task Tickets. By configuring Auto-Assign actions, you can assist the Service Desk Agent who creates the Task Tickets in assignment and routing of the Task Tickets.

Note:

The Auto-Assign Action lookup displays action options available for Task Tickets. Therefore, configuring appropriate Action Options from the Manage Workflow Action section is a pre-requisite to configuring Task Templates with Auto-assign action.

If the Auto-Assign action is specified but the Auto-Assign on Create is not checked, the ticket gets created, but does not get automatically assigned to the designated individual or support group. The Service Desk Agent working on the Parent Ticket can use an Assign All action to manually assign the ticket.

You can configure Task Ticket Templates without configuring auto-assign related actions as well.

Frequently Asked Questions

This section lists questions you may encounter when configuring or managing ticket templates.

How does configuring a ticket template help?

Configuring Ticket Templates eases the effort needed by the users to log the request. As all essential fields can be pre-populated on the ticket template, the effort needed to submit the request is minimal.

Configuring Ticket Template also helps in standardizing the request formation and ensuring that all essential information is captured before the ticket is submitted. This helps expedite the ticket handling process.

Can a ticket template be used for more than one ticket types?

No, a ticket template can be configured for only one Ticket Type. The dropdown list in the Ticket Type field will not allow you to select more than one ticket type.

Can self-service users access ticket templates to create Incident Tickets or Service Requests?

Yes, you can configure ticket templates for Incident and Change Tickets and enable access permission for these templates to Self-Service Group.

The Self Service Users can access ticket templates from the Request Catalog section in the Self-Service User Interface.

What does the checkbox - Override auto-assignment - on a ticket template indicate?

You can use this action if you do not want the ticket template to be matched for Matching Conditions on an Auto-Route.

You can control Assignment of Ticket Templates by setting field values for Assigned to Individual or Group (assigned_contact_id & assigned_group_id).

If the override matching conditions option is not checked, the system will automatically search for Auto-Routes that can be applied to the ticket when the ticket is saved.

If an auto-route matches the conditions on the ticket, the auto-route will get applied and the ticket will be routed to the specified support group rather than honoring the Assigned to specified in the ticket template.

When do I use the "Auto-Assign Action" option? It appears disabled for most ticket templates?

The Auto-Assign Action and the Auto-Assign on Create options are enabled only for Task Ticket Templates. You can set an Auto-Assign Action to be executed on a Task Template when the Task Template is used on a Parent ticket.

If you choose an Auto-Assign action - say Assign to Individual and check on Auto-Assign on Create, the task ticket will get automatically assigned to the Assigned to Individual specified in the Set Field.

Can field values on Ticket Templates be modified by agents and self-service users before submitting a ticket?

Yes; Service Desk Agents and Self-Service Users can modify the fields before submitting the ticket.

A ticket template is meant only to provide a format of the information to be submitted. All visible fields on the template are editable.

What happens if I modify a Ticket Template that is already in use? Will this impact older ticket created using that template?

You can modify the set fields or permissions of an existing task template. The changes will not impact older tickets created using the template. The changes will be reflected the next time the template is used for submitting a ticket.

Can values (set-fields) on a ticket template be carried to a child ticket created out of this ticket template?

Set field values like Description, Details, Affected Services, CCTI, get carried over into the child ticket created out of a ticket logged using a template.

If the same custom fields are available on both ticket types, the custom field values will get carried over into the Child Ticket.

Chapter 22- Manage Task Group

Overview

Task Tickets are created for execution of individual tasks needed to be done towards resolution of an open ticket. Where a single task is to be executed; a task ticket can be created from the Parent by the Service Desk Agent working on the ticket.

When multiple tasks are to be done towards resolution of a ticket; and when these tasks can be identified and pre-defined; a Task Group can be configured and made available. Task Templates can be configured for multiple tasks.

All tasks that need to be done towards completion of one activity can be grouped together into a Task Group.

Task Groups are also related to a specific Ticket type; and can be accessed from the Ticket type that the Task Group is related to.

Create Task Group

The Manage Task Group link under Workflow Tools in the Navigation Menu gives you access to the Manage Task Group form. A list of all active Task Groups will be listed in the table. You can filter the list using the available filters.

To view details on an existing Task Group; click on an item in the list. The details are populated in the form below.

The screenshot displays the 'Workflow Tools (Manage Task Groups)' interface. It includes a 'List Filters' section on the left, a 'Task Group List' table, and a 'Task Group Details' section.

Task Group List:

#	Ticket Type	Task Group Name	Task Group Description
1	Change Request	New User Set Up Tasks	New User Set Up Tasks
2	Change Request	Change Type A Only HW	Change Type A Only HW
3	Change Request	Change Type B HW & SW	Change Type B HW & SW
4	Change Request	Change Type C Only HW	Change Type C Only HW

Records 1 to 4 of 4

Task Group Details:

Task Group #2: Change Type A Only HW

Ticket Type: Change Request | Task Group Name: Change Type A Only HW | Task Group Description: Change Type A Only HW

General Information | Permissions

Task Order	Task Name	Task Priority	Task Status	Task Reason Code	Task Description
Variable: Set Center	Create Home Directory	Medium	New	None	Create Home Dir...
Variable: Set Center: 1	Check Actual configura...	Medium	Queued	Assigned to Individual	Check actual con...
Variable: Set Center: 2	Hardware Change /Upgr...	Medium	Queued	Assigned to Individual	Hardware chn...
Variable: Set Center: 3	Testing after HW upgrade		Queued	Assigned to Individual	Testing of Upgra...

Records 1 to 4 of 4

You can create new a Task Group or modify an existing Task Group by adding or removing tasks from the group. You can also manage the Status of the Task Group (active or inactive).

The fields on Task group; and the main actions to manage a Task Group are listed below.

Field Name	Detailed Description
Ticket Type	You can relate the Task Group to a specific Ticket type. You can choose any one ticket type from the dropdown.
Name	You can assign a name as the Task Group Identifier. This name will be listed in all relevant lists and dropdowns.
Description	You can add a brief description for the task group; indicating what the group is used for.
General Information	You can manage Tasks in the Group. You can either add available Task Templates or Create New Task Template related to the Task Group.
Permissions	You can manage permissions to the Task Group from this tab.
Sort Order	You can specify a Sort Order for the Task Group. Tasks are displayed in the Sort Order when used to create tasks for a ticket.
Unrelate	You can unrelate a Task from the Task Group by taking this action.

Service Desk Agents can create task tickets for a ticket they are working on from the Related Tasks Tab of the ticket. For creating tasks using Templates, Agents can choose to either use specific tasks or use a Task Group. When Service Desk Agents create a task using a Task Group; all tasks in the Task group get automatically created and assigned as per the template.

Manage Task Group Check Points

Some points to remember when configuring Task Groups are:

- A Task Group can be related to only One Ticket type
- Assignment, Set Fields etc. of a Task Group is as per the individual action set on the Task Template.
- Tasks from the same Task Group can be assigned to different Support Groups or individuals.
- Tasks in a Task Group can be done either in a sequence or simultaneously.
- All task ticket in the Task Group created at the same time.
- Tasks are displayed in their Sort Order on the Parent Ticket
- If Auto Assign on Create is not checked for the Task Template; Service Desk Agents can take Assign All action to assign the task tickets as designed.

How Do I

Below are some actions you can take related to reports.

Configure Task Group

You can configure a Task Group out of Task Templates. Task Groups can be configured from the Manage Task Group link under Workflow Tools. To create new Task Groups and view or modify existing Task Groups:

Step 1: Click on the Manage Task Groups link. A list of Active Task Groups will be displayed.

You can modify existing Task Groups or create a new Task Group in the form below. The steps to create a new Task Group are listed below.

Step 2: In the Ticket Type field, select a Ticket Type from the dropdown list. The Task Group can be related to Service, Incident, Problem, or Change Ticket.

Step 3: Specify a Task Group Name in the Name field and provide additional details in the description field. Both fields are required fields.

Step 4: Click on Apply Changes to save the Task Group.

When the Task Group record is saved the General Information Tab displays options to Add Task or Create Task and a table that displays Related Tasks will be displayed. The Permissions Tab also becomes visible on the form.

Step 5: Add Task Templates to the Task Group. If the Task Template that will be part of the Task Group is already configured (in the Manage Ticket Templates form), you can add the template directly. Click on Add Tasks. A list of Task Templates will be displayed.

Select the Task Template you wish to relate to the Task Group.

You can also create new Task Templates to be related to the Task Group by clicking on the Create Task action.

All tasks related to the Task Group will be listed in the table. You can assign Task Order to the Tasks in the Task Group.

Step 6: To assign Task Order, click on the Set Order field next to the Task listed. The Task Order form will be displayed. You can assign an order to the Task in this field.

The Tasks will be listed as per the Task Order.

Step 7: From the Permissions tab, enable permissions to the Task Group. You can assign permissions to users, support groups or roles.

Frequently Asked Questions

This section lists questions and answers to common queries that users may encounter when working with Manage Task Groups.

Why is Ticket Type 'Task' not available when trying to configure Task Group?

Task Tickets are always created out of parent Service, Incident, Problem, or Change Tickets. A task ticket indicates an independent unit of work towards a specified larger activity.

As Task is considered the final point in the work breakdown, you cannot create a Task Ticket as a child to another Task Ticket.

What are the pre-requisites for configuring a Task Group or Task Flow?

You have to configure all required Task Templates and Task Groups that you wish to include as part of a Task Flow. Configuring the actual Task Ticket Template is a pre-requisite to configuring a Task Flow.

A Task Group consists of Individual Task Templates. Configuring Task Templates before configuring a Task Group simplifies the processes of configuring a Task Group; however unlike for Task Flow, it is not mandatory to configure Task Templates before configuring a Task Group.

What does the Task Order in a Task Group indicate?

The Task Order in a Task Group controls the sequence of presentation of the Tasks in a Group. All task templates in the Task Group will be listed in their sort order in the Task Group record. You can modify the Sort Order as appropriate.

The Task Tickets in a Task Group get created together. They are listed according to the set Task Order in the Task Information Tab of the ticket when the Task Group is created as Child to the parent ticket.

How does deleting a task template impact a Task Group to which it is related?

If a task template used on a Task Group is deleted, the task ticket will be removed from the list of tasks. This could affect the completion of the task group or task flow to which the template is attached.

Will I get a warning message when I try to delete a Task Template that is related to a Task Group?

Yes, the system will throw up a warning that the Task Template that you are attempting to delete is related to a Task Group. The template will get deleted if you confirm the delete action.

Chapter 23 – Manage Task Flow

Overview

While Task Tickets are created for execution of individual units of work towards resolution of a ticket; Task Groups are created for a set of tasks done collectively towards resolution of an open ticket.

Some standard requests could be require a series of tasks that need to be executed in a specific order, either one after the other or simultaneously; and when all the tasks are complete; the actual reported issue can be considered as complete.

For example; when a new employee joins an organization; a series of IT related Provisioning tasks could be required. One set of tasks could be related to provisioning a machine, another set could be related to provisioning access to application, a third set of tasks could be validation of the settings. Completion of all tasks successfully will set the request for Provisioning IT for the new recruit.

A Task Flow is configured when a series of tasks need to be executed either in a sequence or simultaneously; and where there is dependency on completion of one task for the execution of the other. A Task Flow can be configured using Task Groups and Individual Tasks.

Create Task Flow

You can access Task Flows from the Manage Task Flow link under Workflow Tools in the Navigation Menu. Clicking on this link displays a list of Active and available Task Flows. You can filter the list using the filters provided. To view details of a Task Flow; you can click on an item in the list; the details get populated in the form below.

You can create new a Task Flow or modify an existing Task Flow by adding or removing Tasks or Task Groups from the Task Flow. You can also manage the status of the Task Flow (active or inactive).

The fields on Task Flow; and the main actions to manage a Task Flow are listed below.

Field Name	Detailed Description
Ticket Type	You can relate the Task flow to a specific Ticket type. You can choose any one ticket type from the dropdown.
Name	You can assign a name as the Task Flow Identifier. This name will be listed in all relevant lists and dropdowns.
Description	You can add a brief description for the task flow; indicating what the group is used for.
General Information	You can manage Tasks and Task Groups in the Task Flow. You can either add available Task Templates or Task Groups to the Task Flow
Permissions	You can manage permissions to the Task Flow from this tab.
Sort Order	You can define the order in which tasks in the task flow are to be executed by setting Sort Order
Action on Success	You can determine the action to be executed when the current task succeeds. You can choose from the available options in the lookup.
Action on Failure	You can determine the next action to be taken if the current task fails. You can choose from the available options in the lookup.

You can assign a Sort order to the Tasks and Task Groups in a Task Flow. Tasks get fired one after the other as per the Sort Order specified. However; all task ticket related to a Task Group Template are created together. Upon completion of all task ticket in the Group; the next Task is initiated.

You can also define Action on Success and Action on Failure of a Task or Task Group in a Task Flow. You can choose a workflow action to be applied on the Parent Ticket if the Task or Task Group is completed successfully or it fails.

Set up Task Flows

Task Tickets in the Task Flow are fired in the sort order determined. Task Flow can be configured using single Task Template(s) and Task Group Template(s). A sort order, determining the sequence in which the tasks need to be executed, can also be defined.

This sequence applies to each Task Template related to the Task Flow; and collectively to all Tasks in a Task Group.

You can also configure a workflow action to be applied on the Parent Ticket (which the Task Flow is applied to) if a Task or Task Group is completed successfully or it fails.

You can choose from available workflow action to get applied as 'Action on Success' and 'Action on Failure' for a Task Template or a Task Group Template.

The Action List lookup displays Workflow Actions that are available to Ticket Type the Task Flow is related to. For example; if the Task Flow is related to Service Requests; Workflow Actions that are applied to Service Requests will be displayed in the Action List.

Based on success or failure of the Task Template; the specified workflow action gets executed on the Parent Ticket. For example; if a Task Flow is applied to a Change Ticket for implementation of some hardware upgrades. Action on success of the final task in the task flow could trigger the moving the Parent Ticket into the next Phase; whereas failure to complete successfully could result in the Parent Ticket being reassigned to the Change Manager.

Manage Task Flow Check points

Some key points to bear in mind when configuring Task Flows are:

- A Task Flow can be related to only one ticket type
- A Task Flow can be configured using individual Task Templates and Task Group Templates.
- Task Tickets in the Task Flow are created as per the Sort Order.
- All Tasks in the Task Group are created together. Completion of all tickets in the Task Group triggers the next task in the Sort Order.
- If action on success and action on failure is defined; the matching workflow action gets applied on the Parent Ticket.

How Do I

Below are some actions you can take related to Task flows.

Configure a Task Flow

You can configure a Task Flow using Task Templates and Task Groups. To view and modify existing Task Flows and to create new Task flow:

Step 1: Click on the Manage Task Flow link in the Workflow Tools section in the Navigation Menu.

The Manage Task Flow form will display a list of all Active Task Flows. You can view and modify existing Task Flows and create new Task Flow in the form below. To create a new Task Flow:

Step 2: Select the Ticket Type from dropdown list in the Ticket Type field. You can choose Service, Incident, Problem, or Change Ticket from the list.

Step 3: Enter a Task Flow Name and provide a Task Flow Description. Both fields are required fields where value is needed for the record to be saved.

Step 4: Click on Apply Changes to save the Task Flow Record.

When you save the Task Flow record, the General Information Tab will display options for you to relate Task or Task Group to the Task Flow.

To relate a Task Group or Task to the Task Flow:

Step 5: Set a Sort Order for the Task to be related. The Sort Order of the Task/Task Group determines the order in which the ticket will be created and assigned as per the template.

Step 6: Select the Task Template or Task Group Template that you wish to relate to the Task Flow. The Lookup will display the Task/Task Group list. Choose the record you wish to relate.

You can relate only one record at a time. You can relate multiple Task/Task Groups to a Task Flow.

Task Flow allows you to configure an action to be triggered on the Parent Ticket if a Task/Task Group fails. You can set Action on Success and Action on Failure of a Task/Task Group in the Task Flow.

To set up Action on Success and Action on Failure:

Step 7: Click on the lookup in the Action on Success or Action on Failure field. The Action list displays a list of all actions that can be taken on the Task Ticket. You can choose an action to be taken if the Task succeeds or the Task Fails.

Step 8: From the Permissions tab, assign permissions for users, support groups or roles for access to the Task Flow.

The task flow can now be used for the related ticket type by the agents and for association with the special function of Auto Create Tasks.

Note:

The Action list displays a list of actions that are available for Task Tickets. You have to configure appropriate Action Options for Task Tickets from the Manage Workflow Action link.

Tasks in a Task Flow get fired as per the sort order. Successful completion of a Task/Task Group will initiate the next Task/Task Group in the Task Flow. This functionality is controlled by specific words appearing in the Reason Code when the Status is set to Resolved/Closed.

The Task flow recognizes a Task as Failed if the Reason Code contains the words DENIED or REJECTED. If neither word is included in the Reason Code, the Task Flow will continue as designed.

You must configure an Action Option for Tasks where execution of the action sets Status as Resolved/Closed and the Reason Code is set as Denied/Rejected for indicating that a Task in the Task Flow has failed.

Frequently Asked Questions

Below are answers to some questions you may have related to Task Flows.

Why is Ticket Type 'Task' not available when trying to configure Task Flow?

Task Tickets are always created out of parent Service, Incident, Problem, or Change Tickets. A task ticket indicates an independent unit of work towards a specified larger activity.

As Task is considered the final point in the work breakdown, you cannot create a Task Ticket as a child to another Task Ticket.

What are the pre-requisites for configuring a Task Flow?

You have to configure all required Task Templates and Task Groups that you wish to include as part of a Task Flow. Configuring the actual Task Ticket Template is a pre-requisite to configuring a Task Flow.

A Task Group consists of Individual Task Templates. Configuring Task Templates before configuring a Task Group simplifies the processes of configuring a Task Group; however unlike for Task Flow, it is not mandatory to configure Task Templates before configuring a Task Group.

What does the Task Order of a Task Flow control?

The Sort Order of a Task Flow controls the order in which task tickets will be created in the Task Flow. Task Tickets in a task flow are fired as per the Sort Order. Successful completion of one task will initiate creation of the next task in the Task Flow.

A Task Flow can be configured using Task Templates and Task Groups. All Task Tickets in a Task Group are created simultaneously. Upon completion of the last Task in the Task Group, the next Task/Task Group is fired.

When do I need to select "Action on Success" and "Action on Failure"?

The function of Action on Success and Action on Failure allows you to define what action is to be taken if a task is successfully completed or if a task fails. The identified Action on Success or Action on Failure gets applied to the Parent Ticket (Service, Incident, Problem, or Change Ticket).

For example, you can specify an Action on Success for a Task Ticket related to a Change ticket as Submit ticket for Approval. Upon successful completion of the Task Ticket, the parent Change Ticket will get submitted for approval.

Similarly; you can specify an Action on Failure for the Task Ticket as Assign to Change Manager. Unsuccessful completion of the task Ticket will cause the parent ticket to get assigned to the Change manager.

Ideally; you must configure Action on Success and Action on Failure when you can predict what action can be initiated on the parent ticket if the task succeeds or fails.

How does deleting a task template impact a Task Flow to which it is related?

If a task template used on a Task Group or Task Flow is deleted, the task ticket will be removed from the list of tasks. This could affect the completion of the task group or task flow to which the template is attached.

Will I get a warning message when I try to delete a Task Template that is related to a Task Flow?

Yes, the system will throw up a warning that the Task Template that you are attempting to delete is related to a Task Group or Task Flow. The template will get deleted if you confirm the delete action.

Chapter 24- Manage Communication Template

Overview

Nimsoft Service Desk can be configured to send and receive communication related to tickets, password notifications, service feedback surveys, SLA target notifications etc. Outgoing communication from the application is managed by using communication templates.

Communication Templates allow users to send out customized, routine communications accurately and with minimal efforts. These templates can be used for sending out Email communication and Phone Communication* where configured.

When a communication template is configured, any variable such as Ticket Number, Assigned to Group, etc. can be inserted as place holders at specific places in the standard text of the Template. The relevant information is derived from the context where the template is actually used for notifications.

For instance, if a Service Request is assigned to a specific Support Group, and a communication template is associated with that action/auto-route, identified recipients are notified about the assignment action by the associated communication template, and place holder values like Ticket Number, Assigned to Group etc. get picked from the context of the ticket.

Communication Templates can also be used for manual notification from a ticket. Service Desk Agents can send manual communication from the ticket. When they choose the Send Mail option for a ticket; they can choose from available Communication Templates as the basis for sending their manual communication.

Communication templates can be flagged as to be used for Email Notification or for Phone Notification* and become available for relevant actions accordingly.

Communication Templates used for Email Communication can be made available in any or all of the supported Locales; thus enabling communication records to be generated and sent in the locale of the recipient.

Create or Modify Communication Templates

You can create Communication Templates from the Manage Communication Template link under Workflow Tools in the Navigation Menu. Clicking on this link displays a list of available Communication Templates.

You can filter the list using the available filter options. To view details of an available template; click on item in the list; and the details get populated in the form below.

You can modify details on an existing communication template; or configure a new Communication Template using the Communication Template form. Some of the fields on the Communication Template form are required fields.

The fields on a Communication Template form and their function is explained below.

Field Name	Detailed Description
Related to Form	A Template can be related to Service Feedback, Service Level Management, Incident, Problem , Change, Task or Service Request Ticket Forms.
Template Name	The Template Name is used to provide a short name to identify the Template
Template Description	The Template Description provides field to give more information about the template
Status	This field displays the current Status of the Communication Template. When you Delete a template; the Status is set to inactive.
Locale	This field allows you to set the Locale of the Communication Template. You select an appropriate option from the Dropdown.
Send To, CC and BCC	These fields are used to populate details of recipients of a communication from a communication template. You can select recipients from the Name Search Lookup or choose 'Add a Field From the Form' option.
Subject	This field can contain a text string with place holders for variable text. The place holders can be added using the Add a Field from the

	Form option.
Message	This field contains the message details and can have a combination of text string with place holders for variable text added using the Add a Field from the Form option.
Notification Method	You can choose whether notification using the communication template is to be sent via Email, System or Phone. If a template is marked as Notification method Phone, it becomes available for Phone Notification. If a template is flagged as Email or System, it becomes available
Reply to Address	This determines the mail address displayed in the From field when the communication is delivered.
Reply to Display Name	This sets the name that will get displayed in the From field when the communication is delivered.

A communication Template can be related to multiple forms; and will be available for being associated with actions related to that form type. For example; if a communication template is related to Service Request and Incident Tickets; the template will be available for relating to Workflow Actions on Service Request and Incident Tickets. However, it will not be available on Change Tickets or on any other form.

Recipients of a communication template can be Contacts, Support Groups or Roles. The Name Search Lookup associated with the Send To, CC and BCC fields allows you to choose recipients. You can also add place holders to draw recipients contextually from the form.

If a communication is set to be delivered to a Support Group, the application will look for contact details for the Support Group. If the Support Group contact is found, the notification gets delivered to the Support Group contact ID. However, if Support Group contact details are not found, the application will find the contact details of individual contacts associated with the Support Group, and the notification is delivered to each individual members contact ID.

You can add fields from the form that the template is relate to as place holders in the recipient details (Send To, CC and BCC) fields, Subject field and in the message body. This enables you to create place holders for variable text; which gets replaced with the actual value from the form in the context in which the communication template is used.

Define Notification Method

The Notification Method defined for a template is a required field on the template. There are three notification methods possible – Email, System and Phone.

To allow notification by Phone, the Notification Method selected on the communication template must be Phone. When notification method selected is System or Email, the communication template becomes available for email notifications.

The email delivery option selected when configuring the communication template- System or Email- determines the email ID to which the communication will get sent. The email ID is picked from the Email details specified for the contact in the individual Contact Record.

When configuring a contact record; the Contact Records Section contains Contact First and Last Name, Email ID, PIN and other relevant details about the contact. Further, the Contact Details tab contains details like Employee ID, Manager, Notification Mechanism and other additional details. Here, you can set notification mechanism as Email; and specify a different Email ID for the contact.

If notification mechanism is set and an ID specified; all notification to the contact is sent to the Email ID set in the Notifications Mechanism Field.

When specifying the Notification Method for a communication template; you can choose to send communication either of the two Email IDs of any contact being notified via the communication template.

If you check on Email - the communication gets sent to the Email ID entered in the contact records section If you check on System- the communication gets sent to the Email ID specified in the Notifications Mechanism field.

Thus, by defining Notification method; you can control the delivery mechanism for the communication being sent out by that particular template.

Note: When the communication template is triggered; it looks for the Notification Method specified for delivery of the communication. If an Email ID is not found in the respective field (corresponding to the Notification Method); the communication will not get delivered to that specific contact.

For enabling SLA Phone Notifications, you will need to buy a license from MIR3. Phone Notification is an external service provided by MIR3, and not a default feature available with Nimsoft Service Desk. Currently Phone Notifications are supported only for SLA Notifications, and not other notifications sent out by the application

Add a Fields from the Form

A communication template has place holders for variable text which can be replaced by related text from the form when the template is used. You can add fields from the form for selecting recipients for a communication (Send To, CC and BCC fields); Subject and Message Body.

The Add Fields From the Form option displays both, Standard Form fields as well as Custom Fields on forms. You can filter the list to view either Form Fields Only or Custom Fields Only or All.

The screenshot shows the 'Communication Template #24: Withdrawn Action Notification' interface. The 'Field List' dialog box is open, displaying a list of fields. The 'Field Name' column lists fields such as 'Action Required (cf_action_required_541)', 'Action Required (cf_action_required_568)', 'Closed By (last_closed_by_name)', and 'Computer Type (cf_computer_type_569)'. The 'Field Type' column shows 'All', 'Form Fields Only', and 'Custom Fields Only'. The 'Field List' dialog box has a 'Search' button and a 'Close' button. A red box highlights the 'Field List' dialog, and another red box highlights the 'Add a field from the form...' button. A third red box highlights the 'Add Fields' button on the right side of the dialog.

The list of fields displayed varies depending on the template field where the place holders are being added.

For example; if you are adding fields from the form in the Send to, CC or BCC field; only those standard form fields related to recipient names will be displayed; whereas when using the action for use in the message section; all relevant standard form fields will get listed.

Where a Communication Template is related to multiple forms; the list of fields displayed will be limited to only those fields that are common to all related forms.

The field from the form creates a place holder; where the information is filled from the context when the communication template is used.

Subject Formatting

Nimsoft Service Desk enables email notifications for transactions on tickets. Notifications are also sent for other forms like Approval Notification to Approvers and Reviewers ; Service Feedback Notifications to identified respondents, Password Reset Notifications etc.

All automatic Notifications sent from the ticket in response to an action applied to the ticket or to auto-routing are managed via communication templates.

Nimsoft Service Desk also allows users to log a request by sending an email to the Support Email ID. Users are also sent email notification from the system upon an action or transaction on a ticket that has been logged on their behalf (or logged by them).

Users can update a ticket by responding to the email notification from a ticket. To ensure that the email response to a ticket gets appended to an existing open ticket; the subject of the communication template has to be appropriately formatted.

Nimsoft Service Desk provides for a series of System Defined communication templates which can be used with various implicit workflow actions and other basic functions. These communication templates can be identified by the negative (-) id associated with the template.

Add Translations

When a new Communication Template is configured, the locale of the template is set as Default. If you want the communication records to be sent to intended recipients in their own locale, you can Add Translations for the communication template for any or all supported locales.

When the communication record is generated using the associated Communication Template, the record is generated in the Default Locale and in each locale of the intended recipient specified in the To, CC or BCC fields of the Communication Template.

When you Add Translation, fields like Related to Form, Template Name, Template Description, To, CC and BCC become Read Only fields. You can modify the Subject and Message fields with translation in the appropriate language.

Making the Default Communication Template inactive will result in all translated templates becoming inactive. You can also choose to make any translated template inactive, without affecting other translations.

System Defined Communication Templates

These communication templates are default notification templates associated with some key Workflow Actions and other transactions in the application, such as client viewable worklogs, change approval pending notification etc.

You can modify details of the system defined communication templates; like change recipient details, modify subject or message details section.

You can also manage Status of the communication template to make the template inactive or Active.

Manage Communication Template Check points

Below are some aspects to check back on when configuring communication templates:

- You can Add a field from the form as place holder for variable text. Token values get replaced from the context of the record when the template is used.
- You can choose to use both standard form fields and custom fields as place holders.

- Communication Templates can be related to multiple forms. When a template is related to multiple forms; only fields common to all related forms are displayed when using Add a field from the Form option.
- The Subject of the template has to be correctly formatted for replies to get updated to open tickets.
- Text in the Communication Templates can be in any language. You can set the Locale for a Communication Template, and thus enable communication records to be generated in the locale of the intended recipient.
- You can have only One Active copy of a Communication Template per Locale.
- You can make inactive copies of a communication template (translation in any locale except default) without affecting the templates of other locales. But if you make the communication template with Default Locale Inactive, all translations will also become inactive.

How Do I

Below are some actions you can take related to Communication Templates.

Configure a Communication Template

You can configure a Communication Template from the Manage Communication Templates link under Workflow Tools. To configure and modify communication templates:

Step 1: Click on the Manage Communication Templates link. A list of Active Communication Templates will be displayed in the list below.

You can modify an existing Communication Template or create a new Communication Template in the form below.

To configure a new Communication Template:

Step 2: From the Related to Form lookup, choose the forms that the Communication Template is related to. A Communication Template can be related to multiple forms listed in the lookup.

When you create a new Communication Template, the Status is set as Active, and Locale is set as Default.

Step 3: Enter a Name for the Communication Template in the Name field, and provide a description. Both fields are required fields.

Step 4: Select recipients of the communication made using the Template. Recipients can be added to Send To, CC or BCC fields.

There are two ways of selecting recipients:

1) You can choose names (Users, Support Groups or Roles). To select recipient names, click on the lookup icon in the Send To, CC or BCC fields. The Name Search will be displayed. You can select recipients from the lookup.

2) You can add recipients contextual to the ticket by Adding Fields from the Form. To add recipients from the form, click on the Add a Field from the Form button.

The lookup will display a list of only those fields on the related form which can be used to add recipients (like Assigned Individual, Assigned Group, Requester etc.). You can filter the list to view only standard form fields and custom fields.

Step 5: Configure the Subject of the communication template. You can choose fields from the form to configure the Subject.

Step 6: Configure the Message Body. You can create a message body as a combination of free text and fields from the form.

Step 7: Choose a Notification Method. This will control which email ID of the recipient the notification gets sent to.

Step 8: You can choose to add Display Address and Display name that will appear in the Receives From field when the communication is sent.

Step 9: Click on Apply Changes to save the Communication Template. The Communication Template will now be available as an Active record.

When the Communication Template is saved, the Permissions tab gets displayed on the form.

Step 10: Enable permissions to access the communication template for users, support groups and roles.

If permission is enabled, the Communication Template will be available for manual communications sent from a ticket, and other actions by the designated user.

Create a Communication Template for multiple Locales

A Communication Template can be configured for each of the supported locales, so that when a communication record is generated, it is sent to an intended recipient in their preferred locale.

For each Communication Template, you can have one copy of the template per locale.

Note: You will first have to create a Communication Template with Locale as Default before creating copies of the template for the other locales.

To create Communication template for other locales;

Step 1: Click on Manage Communication Templates in Workflow Tools.

The Manage Communication Template form will be displayed, with a list of existing Communication Templates.

Step 2: From the list of existing templates, select the template for which you wish to add translation for a different locale.

The form below will get populated with details of the selected record.

Step 3: Click the Add Translations action button.

The Locale field will get enabled, allowing you to choose a locale for the translated Communication Template.

Step 4: Select the locale for the Communication Template from the dropdown list.

The Related to Ticket, Name, Description, To, CC and BCC fields will be Read Only fields. You can modify these fields only in the template with Default locale. When you modify any of these fields in the Default locale, the change automatically gets applied to any available translations.

Step 5: Modify the Subject and Message fields with appropriate translation or text as per the selected locale.

Step 6: Click Apply Changes

A communication template for that locale will get saved. You can follow the same procedure for every locale that you wish to make a translation available for.

Note: You can have only one Active copy of a Communication Template per locale. If you Add Translation and select Locale for the copy same as an existing Active copy, a message asking confirmation to overwrite the existing template will be displayed.

Manage Notifications from a Communication Template

You can configure a Communication Template from the Manage Communication Templates link under Workflow Tools. To configure and modify communication templates:

You can associate two email IDs with a Contact Record.

One Email ID is associated with the Contact Profile. This is the default email ID where all communication from the application is sent to the user.

Another Email ID is associated with the contact record in the Employee Information Section. (This section includes details like Employee ID, Manager and other such details).

In this section, you can configure Notification Mechanism. You can choose Notification Mechanism as None, Email, or Pager. You can add an Email ID in the Pager Email ID field, which can be different from the Email ID in the Contact Profile.

You can manage the email ID to which notification from a Communication Template reaches an intended recipient by specifying Notification Method on the Communication Template.

To set up notifications to reach the Contact Profile Email ID (the default mail ID of the contact), in the Notification Method check box, choose Email. Notifications sent out using the communication templates will be sent to the default Email ID.

To set up notifications to reach the other (Pager) Email ID, in the Notification Method check box, choose System. Email Notification sent using this communication template will be delivered to the Email ID specified as Pager Email ID.

Note: Email ID is not a required field for configuring a contact record. You can choose not to configure an email ID for the Contact. However, not configuring an Email in this field will impact the ability of the contact to receive notifications from the application.

If Notification Method specified is Email and no Email ID is configured in the Contact Profile section, the notification will not be delivered. The communication to the intended recipient will fail.

If Notification Method specified is System, and no Email ID is provided in the Pager Email Id field, the notification will not be delivered. The communication to the intended recipient will fail.

Configure the subject of a communication template

You can configure the Subject of the Communication Template with fields from the form as placeholders in the subject. To configure the Subject with place holders:

Step 1: Click on the Add fields from the Form button in the Subject The Due Date field is displayed field. The lookup will display a list of all fields on the forms related to the Communication Template.

Step 2: Select the field you wish to add to as place holders.

Appropriate special characters will be associated automatically with the field name. This helps define the field as a place holder.

The subject field can be configured as a combination of plain text as well as place holders from the form.

Subject Formatting for Replies to Notifications

Users who receive notifications from the application can respond to the notification if a response to the notification is required. For example consider a notification stating that the ticket has been moved to Pending because information needed to process the ticket is not available.

In such a situation, the recipient of the notification can respond to the notification to provide the missing information. To ensure that response to the notification gets associated with the open ticket, and does not result in creation of a new ticket, special Subject Formatting is required.

The special formatting should be included as the first word/phrase in the Subject.

One formatting style you can use is:

SRQ # followed by case id and ticket id, where Case ID and Ticket ID can be inserted as placeholders from the form.

A Second formatting style you can use is:

Service Request # followed by case id and ticket id; where Case ID and Ticket ID can be inserted as place holders from the form.

You can replace SRQ with INC, PRB, CHG or TSK for Incident, Problem, Change or Task Tickets respectively.

Frequently Asked Questions

Below are answers to some questions you may have related to Communication Templates.

What are the system defined communication templates, and what are they used for?

System defined communication templates are made available for a wide range of commonly used communications.

There are some automatic notifications that are sent by the system for some actions. Take the example of when a workflow uses a special function of Check for Open Tasks. Based on finding the owners of all open task tickets in a ticket related to a global issue get a system defined communication. For such communication needs, system defined communication templates are made available.

System defined communication templates are also made available for standard notifications like approval reminders, service feedback reminders and notifications, password reset notification, etc.

Can I make a system defined communication template inactive or otherwise modify it?

Yes, you can modify a system defined communication template as appropriate, as well as make the template inactive. An inactive template however, will not be available for notifications and communications sent out by the application.

Can I use the same communication template for more than one form?

Yes, a communication template can be used for more than one form. The related to form lookup allows you to choose multiple forms in the lookup.

Can I modify a communication template that is associated with notifications for an auto-route; after it is already in use? What are the implications of such a change?

Yes, you can modify a communication template that is related to an auto-route or workflow action or any other record.

The changes get applied the next time the communication template is used for a notification. Older records are not affected by the change.

What happens if the recipient of a communication sent using a communication template is inactive?

If the recipient of a communication made using a template is inactive, the communication will fail. The communication record will display the delivery status as failed.

What happens if the Group receiving a notification from a communication template is Inactive but some individual member is active?

The communication will be sent out, but will get delivered only to those contacts who are active. Communication to inactive contacts will fail, and you will be notified that the communication could not be delivered to identified contacts.

Will all communication templates be automatically available for all agents?

No, all communication templates will not become automatically available to all Service Desk Agents. Access to communication templates is controlled by permissions assigned to Support Groups, Users and Roles.

A Service Desk Agent can access to all those communication templates for which permission has been directly assigned or inherited via support group or role.

Can a communication be sent by manual action of Service Desk agent using a communication template?

Yes, Service Desk Agents can use communication templates to send manual notification from the ticket. When they click on Send Mail option of a ticket, they can view communication templates related to the ticket form that they have access to.

The Agent can use any communication template listed to send out or schedule the communication.

Can agents modify Communication Templates that they use for manual communication from the ticket?

Yes, agents can modify the communication template before they send out the mail manually. The template is meant only as a format for the agents to follow; it is editable.

Can a communication triggered by an Action Option or an Auto Routing be modified before it is transmitted to the recipients?

A communication template that is associated with an action option or auto-route can be modified; and the changes are visible next time the communication is sent using the template.

However, at the time of execution of an action option or auto-route, the communication templates cannot be modified. This is because these notifications go out without any manual intervention.

Can a Communication template associated with an Action Option or an Auto Routing be deleted?

Yes, you can delete communication template associated with an Action Option or Auto-Route. The status of the communication template will become inactive, and the template will no longer be used for communications. This means that although the template will continue to be listed in the Communications tab of the Auto-Route or Action Option; notification using the template will no longer get sent.

What happens when an Action Option or an Auto Routing is executed and the communication template it triggers has been deleted?

If the communication template is deleted, and an inactive communication is associated with the Action Option or Auto-Route, the communication will not be triggered as communication cannot be sent using an inactive template.

Chapter 25- Manage Workflow Actions

Overview

A workflow is depiction of a sequence of operations that can form a reliable and repeatable pattern for an activity that is being performed. Workflows can be designed to allow systematic performance of an activity based on best practices and industry standards.

The progression of a ticket through its life-cycle is managed by the Workflow Actions configured for different stages of the Ticket. This progression is achieved by configuring Auto-Routes for ticket assignment and Actions Options for moving the ticket into its next stage. For Change Tickets, an additional component of Approvals and approval based actions can be configured.

As Application Administrator, you can configure Workflow Actions to suit the ticket management process specific to your Organization. You can configure Auto-Routes to be applied to a new ticket when it is first created and saved, Action Options to be available for progression of a ticket through a workflow design, and configure approval groups for tickets that need to go through an Approval process.

When a new slice is provisioned or installed, some default ITIL based workflow configurations are enabled for your slice. You can choose to use these workflows the way they are, modify them according to your needs, or start afresh with your own workflow configuration.

This section discusses the available workflow actions as well as ways of configuring and managing the workflow actions for different Ticket types.

Workflow Action Options

An Action Option is a customized action that can be taken on a specified ticket form when the ticket matches pre-defined conditions. Taking an action on the ticket using the action option results in the ticket conditions being changed; fields like Status, Reason Code, Assigned to, etc., get updated as per pre-defined configurations.

A template based communication can also be set off by taking an action on the ticket using an Action Option.

Action Options are available in the Take an Action menu option on the Ticket Toolbar. The Action Options available for a ticket at a particular stage of the Ticket Life Cycle are controlled by the workflow actions configured for the ticket.

The ability for Agents/Analysts or Support Groups to perform an action can also be controlled by granting or revoking Permissions to the Action Option.

For example; consider a Service Request where the Status is 'New' and Reason Code is 'None'. The Take an Action option on the ticket could display Action Options like:

- Accept Assignment
- Take Ownership
- Assign to Group
- Request to Delete Ticket

If the Agent chooses the Action Option of Take Ownership based on the workflow configurations, the Ticket Status could change to 'Active'; Reason Code changes to 'In Progress'; and Assigned to Individual reflects the name of the Service Desk Agent who has taken ownership of the ticket. An email notification could get sent to the ticket requester about the change in status of the ticket.

At this stage, when the Agent working on the ticket wants to move the ticket further along the life-cycle, the Action Options available could be:

- Re-assign within Group
- Escalate to Group
- Pending Additional Information
- Resolved

The Action Options available to the agent change as the ticket conditions change. These Action Options can be configured by the application administrator to manage the workflow of a ticket.

You can manage access to an action option by enabling or disabling permissions to Users, Support Groups, or Roles from the Permissions tab of the action option. The action option will be available only to those Users for whom permission is enabled.

Manage Workflow Action

You can create Action Options from the Manage Workflow Actions link under Workflow Tools in the Navigation Menu. Clicking on this link displays a list of all Active Action Options. You can filter the list using the available filters or search for a specific Action Option from the Search window.

Create Action Option

To view details of a specific Action Option, you can click on an item in the list. The details get populated in the form below. You can also create new Action Options from this form.

Workflow Tools (Manage Workflow Actions)

Filter By: Ticket Type Status Action Type

ID	Ticket Type	Name	Description	Sort Order
23	Incident	Take Ownership of a Queued / Pending Ticket	Take Ownership of a Pending or Queued Ticket assigned to another ag.	31
24	Incident	State Pending for User Call Back	Change Status to Pending for User Call Back from New or Active	61
25	Incident	State Pending for Further Info	Change status to Pending for further information from New or Active	61
27	Incident	Resume work on Pending Ticket	Change status to Pending to Active	61
319	Incident	Create Service Request	Create a Service Request based on incident	88
35	Incident	Create Problem	Create Problem Ticket based on incident Ticket	91
29	Incident	Create Change Ticket	Create Change Ticket based on incident Ticket	110
35	Incident	Close as Resolved	Resolved incident set to Closed as Complete	120
126	Incident	Resolve Incident (High/Critical)	Set status to Resolved pending closure (not auto closed)	130

Records: 41 to 80 of 137

Workflow Action #319 - Accept Initial Assignment

Ticket Type: Incident Special Function: Accept Assignment Name: Accept Initial Assignment Sort Order: 0 Status: Active

Description: Agent accepts incident for initial Diagnosis

Close Ticket Window on Save: Yes No Apply Status To Parent Service Request: Yes No Apply Reason Code To Parent Service Request: Yes No

Matching Conditions: Criteria: ("Status" = "Queued" OR "Status" = "New") AND "Reason Code" = "Initial Assignment" AND "Phase" = "Initial Diagnosis"

Match Type: Include Order: 0

Requester Organization: Requester Site: Requester Location: Source: --Clear--

Requested For Organization: Requested For Site: Requested For Location: Assigned Group: --

Class(es): Category: Type: Item: --

Status: Phase: Reason Code(s): Change Type: --

The main fields in the Manage Workflow Actions form are:

Field Name	Detailed Description
Ticket Type	An Action Option can be related to only one Ticket type. You can choose the ticket form that the action option is related to from the lookup.
Special Function	The special function allows you to automate the workflow action. You can associate a special function to an action option from the Special Functions listed in the dropdown list.
Name	You can specify a name as an identifier for the Action Option. This name will be displayed as the Action Option in the Take an Action dropdown on the ticket where the action is available.
Description	You can add a description which gives Additional Information about the action option.
Sort Order	You can specify a Sort Order for the Action Option. All actions in the Take an Action dropdown will be listed as per the sort order; with a lower order action option being displayed first in the list; or in an Alphabetically ascending order.
Status	This field indicates the current Status of the Action Option. You can make an Inactive action option as active from this field. Only Active Action Options will be available for a ticket workflow.
Applicable to Groups	This field is enabled only when the Special Function 'Assign to Group' is selected for the Action Option. The field name changes to 'Tasks for Auto Creation' when the Special Function 'Auto Create Tasks' is selected.
Close Ticket window on Save	Setting this option to 'Yes' will result in the Ticket Window being closed when the ticket is Saved. Service Desk Agents working on the ticket will need to access the ticket again from the ticket queue to work further on the ticket.

Apply Status to Parent Service Request	This option lets you control action on a Parent Ticket via action on the Child Ticket created off a Service Request. This action available only for Incident, Problem, and Change tickets.

When you click on Apply Changes the Action Option gets created. By default the Status is set to Active. Additional tabs of Matching Conditions, Set Fields, Required Fields, Communications, and Permissions are now displayed on the Action Option form.

You can add appropriate Values into these fields to define when the Action Option can become available (Matching Conditions) and what changes are enabled on the ticket when the action option is used (set fields, Required Fields, and communications). You can manage access to the action option via the Permissions tab.

Special Function

Special Function is a feature that allows you to automate the workflow action by defining an additional action that gets executed when that Action Option is used on the ticket. You can select which Special Function is to get executed by selecting from the available dropdown options.

By default, the Special Function field option displayed is None; meaning no Special Function gets associated with the Action Option.

The Special Functions available are:

- Assign to Individual
- Assign to Group
- Accept Assignment
- Delete Ticket
- Check for Open Tasks
- Move to Case
- Reassign in Group
- Create Service Request
- Create Incident
- Create Problem
- Create Change
- Auto Create Tasks

- Submit for Approval
- Withdraw from Approval.

You can use Special Function to better manage the workflow on a ticket. When the Special Function of Assign to Individual or Assign to Group is selected, the Applicable Groups field gets enabled, and you can select the Group to which the ticket should get assigned.

When the Special Function of Auto Create Tasks is selected, the Tasks for Auto Creation field gets enabled as a Required field. You can select from the available Tasks, Task Groups and Task flows that should get created when the Action Option gets executed on the ticket.

Note: When configuring a Workflow Action Option especially for actions to get executed in response to SLA Phone Notifications, do not associate any Special Function with the Action Option. If selected, the Action Option will not be available when choosing Workflow Actions during the configuration for Response for Phone Notifications.

If a workflow action has Special Functions except None, Auto Create Tasks and Submit for Approval, it will not be available to be associated with an Auto-Workflow Action.

Matching Conditions

The Matching Conditions tab on the Action Option allows you to specify at which stage of the Ticket Life Cycle and during what conditions on the ticket will the Action Option be available. You can configure a matching condition by selecting fields from the ticket and specifying the values on these fields that should be matched to determine whether the Action Option shall be available for the ticket or not.

There can be multiple Matching Conditions for a single action option. Each Matching Condition has its own Sort Order which controls the order in which the conditions get applied to the ticket. You can also specify whether that matching condition is to be included or excluded when making the match.

The screenshot displays the 'Matching Conditions' configuration window. It includes a 'Criteria' text area containing the expression: `(([status] = "Active" OR [status] = "New") AND [in approval phase] = "0")`. Below the criteria are three buttons: 'Apply Changes', 'Create New', and 'Cancel'. At the bottom of the window, there is a 'Match Type' dropdown menu currently set to 'Include', an 'Order' dropdown set to '3', and several input fields for 'Requester Site', 'Requester Location', and 'Source'. A 'Clear' button is located next to the 'Source' field.

The table below identified the fields available on the Matching conditions tab.

Field Name	Detailed Description
Criteria	This field displays the SQL statement that indicates the Values that have been set as matching conditions for the action option. It also displays the Sort Order of the matching condition.
Match Type	You can choose whether ticket with specified Values for fields has to be included when applying the matching condition; or is to be excluded.
Sort Order	You can set a Sort Order for the Matching condition. The matching condition gets applied in the order specified.

The matching conditions tab also displays all the standard fields on the ticket. Some key fields to use when configuring a workflow action are:

- Requester and Requested For Organization, Site and Location,
- Ticket Source
- Ticket Status, Reason Code, and Phase
- Ticket Priority, urgency, impact, and severity
- Ticket CCTI
- Change Type
- Approval Phase, Approval Status, and Approval Type
- In Approval Phase (Yes or No)

You can enter appropriate values that should be present in these standard ticket fields either by choosing Values from the dropdown or manually entering an appropriate value.

In addition to these standard fields, you can also choose Custom Fields on ticket. You can choose up to 6 custom fields as matching conditions for a workflow action. The Custom Fields can be selected from the fields labeled Attributes. The Attribute Value field allows you to set the value that should match for the workflow action to get applied.

You can use an attribute from the available drop down list, such as Department name with an alpha numeric or wild card Attribute value of "BA2%". Similarly you can use attribute values such as " (empty)" for empty custom field, or " | " to indicate a choice such as " A|B"

When the appropriate field value is filled in the Additional Information Tab of the ticket (where Custom Fields are displayed on the ticket), the Workflow action becomes available on the ticket during the appropriate stage of the ticket life-cycle.

You can also configure Workflow Actions to be enabled on ticket logged via email sent to the support ID. These are hidden fields and are not visible on the Ticket form on the GUI. The fields that can be used to configure this are

- Received in Mailbox
- Description

If users in your organization send requests to more than one support ID (for example one support ID for Network related requests, and another for standard user requests), you can configure multiple email boxes for your instance of the application. You can then configure a workflow action to get applied when a mail is sent to one or another mailbox.

You can also configure ticket description (or subject of email) as a matching condition by specifying the description to be matched in the Description field. Thus, tickets logged with that exact Ticket Description (or exact subject in the email); will trigger that workflow action to become available on the ticket.

For each matching condition, you can specify all values that must be considered. By setting appropriate value in Match Type (include or exclude) you can indicate whether the condition should exist on the ticket (include) or whether the condition must not exist on the ticket (exclude).

You can delete a Matching Condition by selecting the matching condition from the Criteria field. A deleted matching condition gets removed permanently from the record.

Thus, you can design a workflow process suited to your organization, and the workflow process suited to your needs.

Set fields

When a Service Desk Agent working on a ticket takes an action on the ticket, this action can be configured to trigger changes in the field values for standard ticket fields as well as ticket Custom Fields.

You can configure the field values to be set on the ticket when an Action Option is used on a ticket. If Set Fields values are configured and when an agent working on the ticket chooses the Action Option from the Take an Action list, the field Values automatically get updated to the values specified in the set fields.

You can define set field values from the Set Fields tab of the Action Option record. The tab displays a table where one column allows you to choose the field value to be set and the other column allows you to set the corresponding field value.

Field to set	Value
Reason Code (ticket_reason_code)	Assigned to Group
Status (ticket_status)	Queued
(cc)_search	

You can modify the Set Field values; add or remove fields from the Set Fields list.

The changes get applied the next time the action option is used on a ticket. Older records do not get impacted by any changes made in the set fields tab.

Required Fields

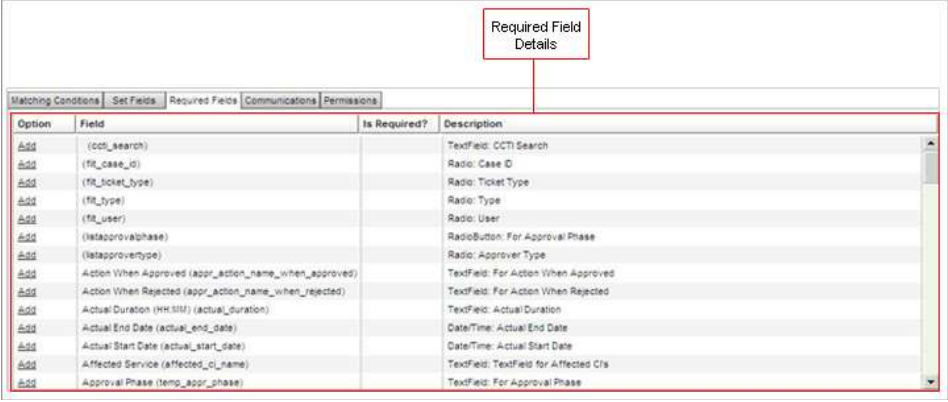
Processing of a ticket requires information to be present in the ticket fields defined. While not all fields are required to be filled in for all tickets, information in some fields could be crucial for further processing of the ticket.

Ensuring that appropriate Values are filled in identified fields would help gather all information needed to process the ticket; as well as to initiate the next set of actions on the ticket.

When configuring a workflow action option, you can mark selected fields on the ticket as Required Fields. The Support Group, Agent/Analyst working in the ticket will be prompted to add value into those fields when they Save the ticket. A message indicating that the selected fields are Required Fields and need appropriate information will be displayed when the ticket is saved without filling in those fields.

The Required Fields tab on the Action Option allows you to specify which fields on the ticket must be marked as Required Fields. This tab displays a list of all fields on the ticket. This includes both standard fields on the ticket as well as custom fields on the ticket.

The table allows you to view all the fields on the form and corresponding field description. By clicking on 'Add'; you can mark the field as Required field. The Required Field, Yes/No, displays whether the field is required or not. You can remove the required field tag from the field by clicking on the 'Remove' action.



Option	Field	Is Required?	Description
Add	(ccs_search)	☐	TextField: CCT Search
Add	(tr_case_id)	☐	Radio: Case ID
Add	(tr_ticket_type)	☐	Radio: Ticket Type
Add	(tr_type)	☐	Radio: Type
Add	(tr_user)	☐	Radio: User
Add	(dateapprovalphase)	☐	RadioButton: For Approval Phase
Add	(dateapprovaltype)	☐	Radio: Approver Type
Add	Action When Approved (appr_action_name_when_approved)	☐	TextField: For Action When Approved
Add	Action When Rejected (appr_action_name_when_rejected)	☐	TextField: For Action When Rejected
Add	Actual Duration (HH:MM) (actual_duration)	☐	TextField: Actual Duration
Add	Actual End Date (actual_end_date)	☐	DateTime: Actual End Date
Add	Actual Start Date (actual_start_date)	☐	DateTime: Actual Start Date
Add	Affected Service (affected_ci_name)	☐	TextField: TextField for Affected CIs
Add	Approval Phase (temp_appr_phase)	☐	TextField: For Approval Phase

You can add or remove required fields associated with an action option. The change gets applied the next time the action option becomes available on the ticket. Older records are not affected by the modifications to the Required Fields tab.

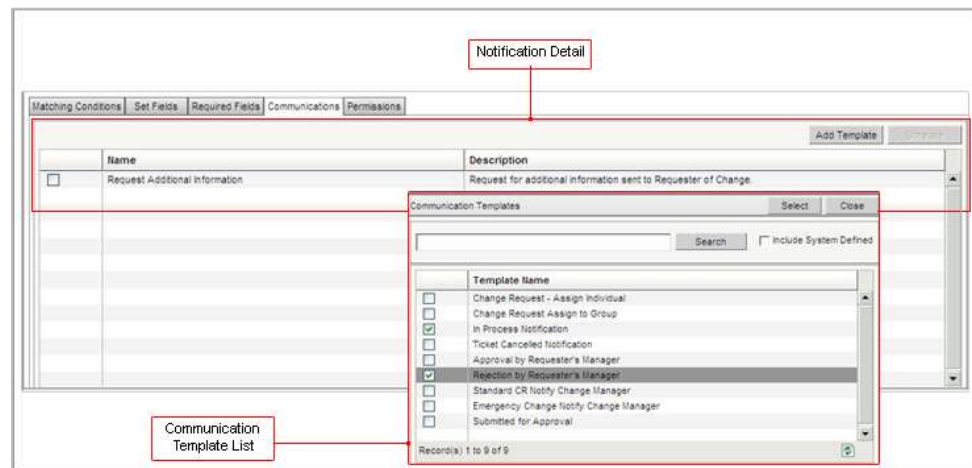
Manage Notifications

A workflow action on the ticket can be configured to send out automatic Notifications to identified recipients. You can relate Communication Templates to the Action Option from the Communications tab.

A notification based on the communication template, will get sent out to recipients identified in the communication template regarding the action that has been performed on the ticket.

This tab displays a list of Communication Templates associated with the action option. You can add new communications using the Add Template action button. All Communication Templates that are related to the Ticket type which the action option is related to, will get displayed in the lookup.

You can filter the list to include or exclude system-defined communication templates.



Multiple templates from the list can be selected and added to the action option. You can add new Communication Templates to the action option or remove existing template to discontinue the notification.

The changes get applied next time the action option gets applied to the ticket. Older records are not impacted by any modifications to the Notifications tab.

Manage Permissions

Access to all workflow action options can be managed by assigning or revoking permissions to the action option from the Manage Permissions tab.

For example, you might want to restrict access to an action option like Create Problem Ticket to a Level 2 or Level 3 Support Group, and not allow Level 1 Support Group to access this action option. Thus, even if all matching conditions get applied to the ticket, the action to create Problem Tickets becomes available only to the Level 2 or 3 Support Group.

Controlling permissions to Action Options allows you greater control on what actions can be taken by which support group.

An Action Option becomes available only to a support group that has been granted permission to the item. You must therefore remember to assign permission to an action option to all appropriate support groups, roles and individuals.

Manage Action Options Check Point

The key points related to workflow Action Options are:

- An action option is available only when the ticket meets the matching conditions specified on the action option.
- If no matching conditions are specified, the Action Option becomes available on all ticket of the selected Ticket Type.
- Action Options available on a ticket are displayed in the Take an Action option on the ticket toolbar.
- Access to an Action Option is controlled by Permissions.
- Inactive Action Options will not be available for a ticket Workflow Process.
- If an Action Option is not configured correctly, the action will not get executed. An error message will be displayed.
- If set-field values are incorrectly specified, the field value will not get updated when the ticket is saved.
- Modifications to an action option do not impact older records. They are applied next time the action option gets applied.

How Do I

Below are some actions you can take related to Workflow Actions

Configure a Workflow Action Option

Processing of a ticket through different stages, from creation of the ticket through to its resolution and closure, is managed by configuring Workflow Action Options.

Action Options applied to the ticket progress the ticket from one stage to another as per the workflow design. Action Options that are available on the ticket at a particular stage can be managed by configuring matching conditions.

To access the Action Options form:

Step 1: Click on the Manage Workflow Action link under Workflow Tools in the Navigation Menu.

A list of Active Action Options will be displayed in the table. You can view and modify details on an existing Action Option or create new Action Options in the form below.

To create a new Action Option

Step 2: Select Ticket Type from the dropdown list. You can relate an Action Option to any one ticket type.

Step 3: You can choose a Special Function if you want to associate a Special function with the Action Option. This is, however, not a required field.

Step 4: Enter a Name for the Action Option in the Name field, which is a required field.

The Name will appear in the Take an Action dropdown list when the Action Option becomes available on a ticket based on its Matching Conditions.

You may choose to enter a detailed description for the Action Option if necessary, though this is not mandatory. You can also choose a Sort Order for the Action Option.

All Action Options will be listed either in the designated Sort Order or in an Alphabetic Order in the list and on tickets.

Step 5: Click on Apply Changes to save the Action Option record.

The Matching Conditions, Set Fields, Required Fields, Communication and Permissions tab now get displayed on the form. You can now configure aspects like when the Action Option becomes available, what happens when the Action is executed and control access to the Action Option.

An Action Option can be configured to be available to a ticket based on matching conditions like status, reason code, phase, CI, assigned to group etc.

To configure Matching Conditions:

Step 6: In the Matching Conditions tab, configure Conditions which should be matched on a ticket to control availability of an Action Option.

You can configure Matching Conditions as Include or Exclude statements.

In the relevant field (like Requester Name, Received in Mailbox etc.); add the values that should be included or excluded for matching the ticket conditions.

You can configure multiple matching conditions to control applicability of an Action Option. Both standard ticket fields and custom field values can be used as matching conditions.

Once the Action Option gets applied to a ticket, you can configure other actions that should happen on the ticket.

In the Set Fields Tab, you can set field values that should get set when the action option gets applied to the ticket.

Step 7: In the Set Field tab, you can configure the Field Values that are to be set on the ticket when an Action using the Action Option is executed.

Set Fields can be configured to set values for Standard Ticket fields (like Assigned to Individual/Group, Priority, Urgency etc.) and for Custom Fields on the ticket.

Step 8: Some information could be critical to further processing of the ticket. In the Required fields tab, you can select the ticket field where value has to be entered before an action is executed using the Action Option.

You can choose fields like CCTI, Worklog, and other Custom fields as Required Fields, as merited by the requirements of processing the ticket.

You can now configure automatic notifications to be sent out when an action is executed on the ticket.

To relate communication templates to the action option:

Step 9: Click on the Communications Tab to view any related Communication Templates and to relate Communication Templates to the Action Option.

Step 10: Click on the Add Template option in this tab. A list of active Communication Templates related to that form type will be displayed.

By default only customer configured Communication Templates will be displayed. Check the Include System Defined checkbox to view a list of all custom defined and system-defined Communication Templates.

Step 11: Select one or more relevant templates from the list and click on Select.

The communication templates will get related to the Action Option. When the action is executed, automatic notifications will get sent to recipients identified on the template(s).

You can now manage access to an Action Option for Contacts, Support Groups and Roles.

Step 11: Click on the Permissions tab to view a list of contacts who have been given access to an Action Option.

The Administration Group has default access to the Action Option. From the Permission Editor (using the Mange Permissions action button), add users, groups and roles to the list of Contacts with Permissions to the Action Option.

The Action Option will now become available on all tickets with Matching Conditions. Execution of the Action Option will trigger the train of associated actions on the ticket.

Note: If no Matching Conditions are set for a Workflow Action, the Action Option will be available for all tickets of that ticket type.
If multiple Matching Conditions are configured, the Action Option will become available only when ALL conditions match.
When you Set Fields, you must exercise due caution to choose values that you can select from dropdown or lookup lists. If irrelevant value is set, the field value will not get applied when the ticket is saved.

Manage Matching Conditions

You can configure Matching Conditions for controlling applicability of an Action Option on a ticket at a particular stage, and for Auto-Routes applied for routing of new tickets.

The Matching Conditions tab gets enabled on an Action Option or Auto-Route after the record is saved.

To configure Matching Conditions:

Step 1: In the Matching Conditions form section, select Match Type as Include or Exclude from the dropdown list.

If the Match Type is INCLUDE, the Action Option/Auto-Route will get applied if the identified conditions exist on the ticket.

If the Match Type is EXCLUDE, the Action Option/Auto-Route will get applied if the identified conditions DO NOT EXIST on the ticket.

Step 2: Select a Sort Order for the Matching Condition statement.

Where more than one statement is configured as Matching Condition, the system will match for ALL identified conditions one after the other in the Sort Order indicated.

Step 3: Choose from the ticket field which you wish to use as Matching Condition; for example, Requester Organization/Source/Priority, etc.

Step 4 Below the field name, enter the value which should be matched for; for example, if the Field Name chosen as Matching Condition is Status, you can enter New/Pending/Active etc. in the field below.

You can configure one statement comprising of more than one field. For example, you can configure a statement which says "Status =Active OR New & Phase = Technical Approval & Reason Code = Submitted for Approval

Step 5: Click on Apply Changes to save the Matching Condition.

After one Matching Condition is saved, you can configure a second statement in the same way.

Matching Conditions can be configured using Standard Ticket Fields as well as Custom Fields on tickets. The fields Attribute 1 to Attribute 6 (with corresponding Attribute Value) let you set up Custom Fields as Matching Conditions.

You can also use the mailbox in which the mail was received and the Subject of the Email (which get logged as Ticket Description when the ticket is created) as Matching Conditions.

Note: If no Matching Conditions are configured, the Action Option/Auto Route gets applied to all tickets of the related ticket type. You have to exercise due caution when entering field values as Matching Conditions. If an incorrect value (like a wrong spelling) is entered, the Action Option/Auto Route will not get applied to any ticket.

Use Special Function in Action Option

Special Functions is used to enable a workflow action option to trigger off an automatic action on the ticket when the action option gets applied to a ticket.

For example, if you configure an Action Option to "Request to Delete Ticket" which gets applied when Ticket Status is Resolved and Reason Code is Duplicate ticket.

You can configure a Special Function "Delete Ticket", so that when the Request to Delete Ticket action is executed on a ticket, the Delete Ticket Special Function leads to the ticket being deleted.

The special function automatically triggers additional chores to be performed when the Action Option is executed on the ticket.

To configure an Action Option with Special Function:

Step 1: Click on Manage Workflow Actions link under Workflow tools to view the Configure Workflow Action form.

Step 2: Select Ticket Type from the dropdown list to select which ticket type the Action Option applies to.

Step 3: In the Special Function field, choose the Special Function you wish to associate with the Action Option.

Step 4: Enter a Name for the Action Option, which is a required field.

You can add description and Sort Order if necessary; however, you may choose not to modify values in these fields as they are not required fields.

Step 5: If you have chosen Special Function as Assign to Group, the Applicable Groups field will be enabled. In this field, select the Support Group to which the ticket must get assigned when the Action Option gets applied to the ticket.

If you have chosen the Special Function as Auto-Create Tasks, this field name changes to Tasks for Auto-Creation and the field becomes a Required field. You have to choose the Tasks to be created when the Action Option is applied on the ticket.

Step 6: Click on Apply Changes to save the Action Option.

You can now configure Matching Conditions on the Action Option, configure set fields, required fields, and take other actions to make the Action Options available to relevant users.

Note: Special Function can be used when the action is frequent, repetitive and fairly predictable in nature. It removes the need for manual action for very repetitive tasks where human intervention will have little value.

Configure Workflow Action or Auto-Route for Emails

You can configure Auto-Routes for new ticket to be routed to an identified support group based on the Email ID to which the ticket was sent. You can also configure Auto-Routing based on Subject of the Email.

To configure an Auto-Route based on the email ID the mail was sent to, or the Email Subject field:

Step 1: Configure the Auto-Route as normal with Related Ticket Type and Auto Route Name.

Add description and Sort Order to the Auto-Route as appropriate.

Step 2: Click on Apply Changes to save the Auto-Route.

The Matching Conditions, Set Fields, Communication and Time tab now get enabled on the Auto-Route.

Step 3: Create the Matching Condition on the basis of which the Auto-Route should get applied.

In the Match Type say Include.

In the fields section below, where you can choose fields and values as Matching Conditions, there are two fields - Received in mailbox and Description.

Step 4: To configure email ID as the Matching Condition; enter the Email ID to which the Email Request will be sent by the requester for that request.

Step 5: To configure Subject of the Email as Matching Condition, in the Description field enter Description as Matching Condition.

The requests from end users can thus be Auto-Routed by setting Matching Conditions as the Email ID to which the ticket is sent or the Ticket Description (the subject of the Email sent by the requester).

Note:

Multiple Email IDs can be configured for your Slice when your Slice is Provisioned. This is taken up by the Product Support Team. The Email ID used in Matching Condition must be configured for your Slice.

The Subject has to be an exact match for the Auto-Route to get applied. Spelling or other errors will mean that the Auto-Route will not get applied.

Subject or Received in Mailbox can also be used as fields for configuring Workflow Action Options.

Frequently Asked Questions

This section lists possible questions you may have related to managing Workflow Actions.

Can one action option be related to more than one ticket type?

No, a workflow action option can be related to only one ticket type. The drop down list will not allow you to select more than one ticket type.

What does the Special Function field control? When should I configure Special Functions for a workflow action?

Special Function is an option that allows you to initiate some automated action when an action option is applied to the ticket. Execution of the action option will automatically trigger the action associated with the special function.

The dropdown list associated with the Special Function field displays a list of automated actions that can be applied to the ticket when the Action Option is executed. Some special function options allow you to create Child Ticket from an open ticket when the action is executed; set assignment of the ticket; etc.

The Special Function Check for Open Tasks allows you to set an action that can be applied when a Global Issue is being resolved. This action enables you to ensure that all child Task Tickets associated with tickets Related to the Global Issue are closed before the parent ticket that is related to the Global Issue is closed.

The Special Function of Auto-Create Tasks allows automatic creation of task tickets when the associated action option is executed. Using this eliminates the need for the Service Desk Agent working on the ticket to manually create task tickets when the ticket reaches the appropriate stage or condition.

You can use Special Function for an Action Option where you want the Action Option to execute another associated action. It is not a Required field, and can be used if the workflow action merits inclusion of a Special Function.

Can I add a new special function to the list available in the dropdown?

No; you cannot add a new Special Function to the list. However, from time to time, new Special Functions get added to the list to accommodate enhanced functionality related to workflow action options.

Can an Action Option be created without specifying a Matching Condition? How could this affect the workflow configurations?

You can configure an Action Option without creating any Matching Condition for it. If you don't specify matching conditions for a workflow action option, the action option will be available for all tickets of the Related Ticket Type.

An Action Option becomes available on a ticket based on Matching Conditions. If no Matching Condition is indicated, ALL Tickets match the condition for the Action Option. Therefore the Action Option will be available on the related ticket type at all stages of the ticket life-cycle.

What does the sort order control in the workflow action?

The Sort Order of a Workflow Action Option controls the order in which the record will be displayed in the list of available Action Option in the Take an Action option on the ticket.

An Action Option with a lower Sort Order will be displayed first; this is followed by Action Options with higher Sort Orders.

What does the Order of the Matching Condition SQL control?

The Order of the Matching Condition indicates the sequence in which the Matching Condition gets applied by the system. When a ticket is being matched for Matching Conditions of an Action Option, ALL Matching Conditions are matched one after another as per the Order indicated. You can change the Order without affecting the end result of the execution of the action.

You don't have to specify an order for the Matching Conditions. By default, the Order 0 gets applied.

How can two conditions be linked with "AND" operator?

Two conditions get linked with an AND operator when two or more Conditions are specified as EXCLUDE statements. For example, you may want to construct a matching condition where the Action Option should not get applied to a ticket if Status is New AND Priority is High AND Urgency is Critical.

Two or more conditions also get linked with an AND Operator when One statement is an INCLUDE statement and another statement is an EXCLUDE Statement.

Can there be three or more conditions linked with "AND" operator or OR Operator?

Yes, you can configure Matching Conditions where three or more conditions are linked with AND Operators (Exclude Statement). You can also configure a Matching Condition where three or more statements are linked with OR Operator (Include Statements).

You can also configure matching conditions where some statements are linked with AND Operators and some are linked with OR Operators. In such a condition, all the Include statements will be linked to the Exclude statements with an AND Operator.

How does modifying an Action Option impact existing open tickets where the workflow was applied?

There is no impact on records where an action option has already been applied. Once the Action Option is applied to a ticket, the related aspects like Set Field values are set and notifications get sent.

What will happen if I change matching conditions on a action option that is already applied to tickets?

Changing matching conditions on an existing Action Option does not impact records where the Action Option has already been applied. The Action Option will not be available to other tickets with the older matching conditions. It will be applied on tickets that match the new Matching Conditions specified on the Action Option.

Will adding new workflow actions impact existing tickets; or will they only get applied to tickets created after the workflow action was configured?

An action option will get applied to all tickets that match the conditions of the ticket based on the Matching Conditions configured on the Action Option. This includes tickets created before the Action Option is configured.

If the conditions on an existing ticket fit the Matching Condition of a newly configured Action Option, it will be available on the ticket for choosing an action for the ticket.

What happens if I change the set-field values after a action option has already gotten applied?

Changing the Set Field values or Required Fields for an Action Option does not impact older tickets where the Action Option was applied.

When the Action Option is executed next, after modification, the Set Field values will be applied as per the new configuration; and the new Required Fields will be imposed.

Can multiple communications get sent from the same action option?

Yes, you can associate multiple communication templates to send out multiple notifications when an Action is executed via an Action Option. The communication tab will list all communication templates related to the Action Option.

Chapter 26- Manage Auto-Routes

Overview

Tickets logged in Nimsoft Service Desk need to be assigned to specific support group or individual for appropriate action towards action and Resolution of the ticket. The default assignment group for a particular ticket type is set up when managing Ticket Modules and setting up basic ticket functionality.

You can configure default assignment group from Slice Parameter for each ticket type; for example, SRQ_DEFAULT_ASSIGNMENT_GROUP or INC_ASSIGNMENT_GROUP. As per the defaults set, a ticket will get assigned to the default group identified.

This however; could add to the time taken for working on and resolving the ticket because the default group would need to look through the ticket, identify which support group or support individual can work on the request and assign the ticket to that support group or individual.

Auto-Routes are configured to automate the process of assignment of a new ticket to specific group based on specific criteria. By setting up auto-routes, new tickets can get assigned to a specific individual or support group based on matching conditions specified on the auto-route.

For example, consider an Incident ticket that is logged to report the failure of a hardware component. By default the ticket could get assigned to a Level 1 support group (if specified in the slice configuration).

Thus, A Service Desk Agent in the Level 1 support group would take ownership of the ticket, understand the request, and then manually assign the ticket to a Hardware Support Group.

To speed up the support Process, and ensure that the ticket gets assigned to the right support group at the first instance, you can configure an auto route for tickets having Matching Conditions (for example Class = Hardware) to be auto-routed to the Hardware Support Group.

You can configure auto-routes for different Ticket types; and for different Matching Conditions on a ticket. An auto-route can be configured to automatically set field values and initiate communications with identified Stakeholders.

You can also configure a schedule for an auto-route where the Routing can be managed according to the support group Business Hours. This is especially useful where there are multiple support groups handling the similar kind of requests from geographically diverse locations.

Manage Auto-Routes

You can configure and manage Auto-Routes from the Manage Auto-Routes link under Workflow Tools in the Navigation Menu. The Manage Auto-Routes form displays a list of all active Auto-Routes configured. You can filter the list using available filters and search for a specific auto-route using the search window.

To view details of an existing Auto-Route and modify existing auto-route, you can click on an item in the list. The details get populated in the form below. You can also create new Auto-Routes using this form.

The screenshot shows the 'Manage Auto-Routes' interface. On the left, there are three red boxes with labels: 'List Filters', 'Auto Route List', and 'Auto Route Details'. The main area contains a table of auto-routes and a detailed form for one selected route.

ID	Ticket Type	Name	Description	Sort On
27	Incident	Incident from T101 to C42 Support inc	Assign Incident from T101 to C42 Support inc	4
32	Service Request	Create SRG for Incident & make from T101 and o	Service Requests are created from 8 daily coming into system. 24x7 Best SRG By	5
33	Service Request	T101 SRG Service Request to T101 SRG L1	Class Engineering (SRG) Service Requests assignment to Internal SRG Support L1	4
34	Service Request	T101 SRG Service Request to T101 SRG L1	T101 SRG Service Request to T101 SRG L1	5
37	Service Request	T101 Product Info Service Request to T101 Prod	T101 Product Info Category Service Request to T101 Product	6
41	Service Request	Service Request from T101 Singapore to India L1	Assign Service Requests from T101 Singapore to Best SRG India L1 Class and T101	6
42	Service Request	Service Request from T101 London to India L1	Assign Service Requests from T101 London to Best SRG India L1 Class and T101	6
43	Service Request	Service Request from T101 Outpost to India L1	Assign Service Requests from T101 Outpost to India L1 Class and T101	6
44	Service Request	Service Request from T101 Hungary to India L1	Assign Service Request from T101 Hungary to India L1 Class and T101	10

Records: 1 to 10 of 10

Auto-Route #4 - Incident from T101 to C42 Support inc

Ticket Type: Incident
Name: Incident from T101 to C42 Support inc
Description: Assign Incident from T101 to C42 Support inc
Matching Conditions: (SRG) Support inc
Filters: (SRG) Support inc
Requester Type: Incident
Requester Organization: T101
Requester Site: T101
Requester Location: T101
Requester Per Site: T101
Requester Per Location: T101
Requester Per Organization: T101
Assigned Office: T101

Create Auto Route

The main fields on the Auto-Routes form are listed below.

Field Name	Detailed Description
Ticket Type	An Auto-Route can be related to only one ticket type. You can select a ticket type from the dropdown list in this field.
Name	This field allows you to specify a name as the identifier for the

	auto-route.
Description	You can provide more information about the auto-route and its applicability in this field.
Sort Order	You can assign an order for the auto-route. Where multiple auto-routes get applied to the ticket, Sort Order becomes important as the Auto-Route with the lower sort order will get applied to the ticket in this situation.
Status	This field displays the current Status of the Auto-Route. Deleting an auto-route makes it Inactive. You can set an inactive auto-route as Active from this field.
Auto-Workflow Action	This field is enabled after the auto-route is saved. You can choose a workflow action that will get executed when the auto-route gets applied to the ticket. The lookup displays Workflow Actions related to the same Ticket type as the Auto-Route. Only those Workflow Actions with Special Function as 'None', 'Auto Create Tasks' or 'Submit for Approval' will be displayed in the lookup. If a Workflow Action has any other Special Function associated with it, the Action Option will not be displayed here

You can enter the appropriate values into the different fields above. When you save the record by applying changes, the auto-route record is saved. The Auto-Workflow Action field gets enabled.

Additional tabs of Matching Conditions, Set Fields, Communications, and Time are enabled on the auto-route form. You can specify matching conditions when the auto-route should get applied, specify field values to be set when the auto-route is executed, and associate communications to be sent out when the auto-route gets applied. You can also associate a schedule with the auto-route from the Time tab.

Matching Condition

The Matching Conditions tab on the Auto-Route can be configured in the same way as configuring matching conditions for Action Options. You can specify the conditions on the ticket that should be matched for the auto-route to get applied.

You can configure a matching condition by selecting fields from the ticket and specifying the values on these fields that should be matched for the auto-route to get applied.

You can configure multiple Matching Conditions for a single auto-route. Each Matching Condition has its own Sort Order which controls the order in which the conditions get matched with the ticket conditions.

You can also specify whether that matching condition is to be included when making the match or it is to be excluded.

The table below identified the fields available on the Matching Conditions tab:

Field Name	Detailed Description
Criteria	This field displays the SQL statement that indicates the values that have been set as matching conditions for the auto-route. It also displays the Sort Order of the matching condition.
Match Type	You can choose whether tickets with specified Parameter Value have to be included when applying the Auto route or are to be excluded.
Sort Order	You can set a Sort Order for the Matching condition. The matching condition gets applied in the Sort Order specified.

The matching conditions tab also displays all the standard fields on the ticket. Some key fields to use when configuring an Auto-Route are:

- Requester and Requested For Organization, Site and Location,
- Ticket Source
- Ticket Status, Reason Code, and Phase
- Ticket Priority, urgency, impact, and severity
- Ticket CCTI
- Change Type
- Approval Phase, Approval Status, and Approval Type
- In Approval Phase (Yes or No)

You can enter appropriate values that should be present in these standard ticket fields either by choosing Values from the dropdown or manually entering an appropriate value.

In addition to these standard fields, you can also choose Custom Fields on ticket. You can choose up to 6 custom fields as matching conditions for a workflow action. The Custom Fields can be selected from the fields labeled Attributes. The Attribute Value field allows you to set the value that should match for the Auto-Route to get applied.

You can use an attribute from the available drop down list, such as Department name with an alpha numeric or wild card Attribute value of "BA2%". Similarly you can use attribute values such as " (empty)" for empty custom field, or " | " to indicate a choice such as " A|B"

When the appropriate field value is filled in the Additional Information Tab of the ticket (where Custom Fields are displayed on the ticket), the Auto-Route becomes available on the ticket during the appropriate stage of the ticket life-cycle.

You can also configure Auto-Routes to be triggered on tickets logged via email sent to the support ID. The fields that can be used to configure this are:

- Received in Mailbox
- Description

These are hidden fields, not visible directly on the ticket form.

If users in your organization send requests to more than one support ID (for example one support ID for Network related requests, and another for standard user requests), you can configure multiple email boxes for your instance of the application. You can then configure an Auto-Route to get applied when a mail is sent to one or another mailbox.

You can also configure ticket description (or subject of email) as a matching condition by specifying the description to be matched in the Description field. Thus, tickets logged with that exact Ticket Description (or exact Subject in the email); will trigger the appropriate Auto-Route, and the ticket gets assigned to an appropriate support group.

For each matching condition, you can specify all values that must be considered. By setting appropriate value in Match Type (include or exclude) you can indicate whether the condition should exist on the ticket (include) or whether the condition must not exist on the ticket (exclude).

You can delete a Matching Condition by selecting the matching condition from the Criteria field. A deleted matching condition gets removed permanently from the record.

Thus, you can design Auto-Routes matching factors like Support Group Business schedule and according to the needs of your organization.

Set Fields

An Auto-Route can be configured to trigger changes in the field values for standard ticket fields as well as ticket Custom Fields. When a ticket is auto-routed based on ticket Matching Conditions, the ticket gets assigned to the specified group and the field values are set according to the pre-configured values.

If Set Fields values are configured, the Auto-Route triggers assignment of the ticket to the specified support group and the field values automatically get updated to the values specified in the Set Fields.

Set Field Details	
Field to set	Value
Reason Code (ticket_reason_code)	Assigned to Group
Status (ticket_status)	Queued
To add another field, select it from the drop-down menu and click on Add.	

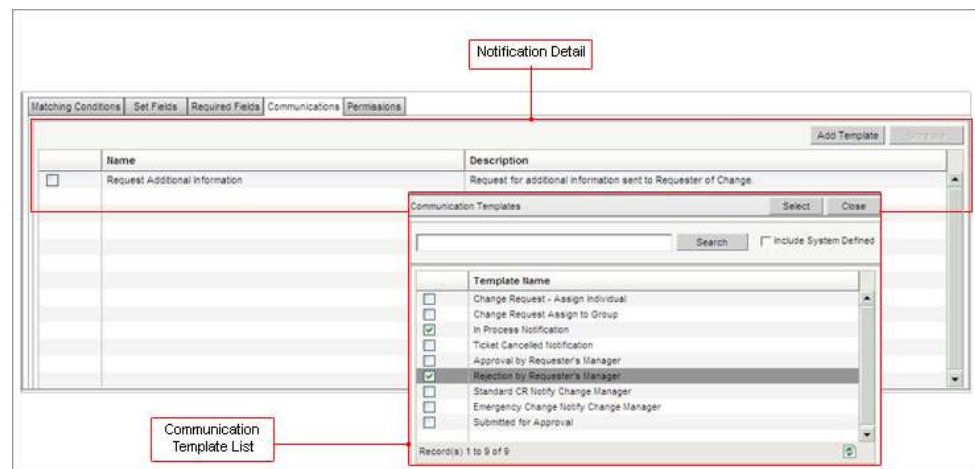
You can define set field values from the Set Fields tab of the Action Option record. The tab displays a table where one column allows you to choose the field value to be set; and the other column allows you set the corresponding field value.

You can modify the Set Field values, or add or remove fields from the Set Fields list. The changes get applied the next time the action option is used on a ticket. Older records do not get impacted by any changes made in the set fields tab.

Manage Notifications

An auto-route can be configured to send out automatic Notifications to identified recipients. You can relate communication templates to the Auto-Route from the Communications tab. A notification, based on the communication template, will get sent out to recipients identified in the communication template regarding the auto-assignment of the ticket.

This tab displays a list of Communication Templates associated with the auto-route. You can add new communications using the Add Template action button. All communication templates that are related to the ticket type which the auto-route is related to, will get displayed in the lookup. You can filter the list to include or exclude system-defined communication templates.



Multiple templates from the list can be selected and added to the auto-route. You can add new Communication Templates to the Auto-Route or remove existing template to discontinue the notification. The changes get applied next time the auto-route gets applied to the ticket. Older records are not impacted by any modifications to the Notifications tab.

Auto-Route Schedule

Auto-Routes are established primarily to ensure that tickets are assigned to a support group that can work on the ticket. Specialized Support Groups usually work only during stipulated Business Hours. Assignment of a ticket outside of these business hours could lead to the delays in working on the ticket. Large support Organizations could also have Support Groups at geographically diverse locations.

To make auto-routes more meaningful by taking into account support group Business Hours and geographical diversity; Schedules can be associated with an auto-route. You can manage the auto-route schedule from the Time tab on the auto-route.

From this tab, you can specify a start and end date; and start and end time for the auto-route. You can associate a time-zone to the auto-route to specify the time to which the auto-route gets applied.

The Repeat pattern of the auto-route controls which days of the week the auto-route gets applied.

You can also associate a Holiday Group to the auto-route. The auto-route will not get applied on the days included in the Holiday list. Similarly, if you want to configure an auto-route to get applied only on Holidays; you can select the 'Run only on Holidays'; this would ensure that the Auto-Route will get applied only on the holidays in the Holiday list.

Thus by associating time to the auto-route, you can create meaningful auto-routing of tickets.

Manage Auto-Route Check Points

The key points related to managing auto-routes are:

- An auto-route gets applied only when the ticket meets the Matching Conditions specified on the Auto-Route.
- The auto-route gets applied only when the ticket is saved for the first time. All subsequent assignments have to be done manually.
- Where multiple auto-route meet the ticket matching condition, the auto-route with the lowest Sort Order gets applied.
- If override auto-route action is specified on a ticket template, the auto-route will not get applied to the ticket.
- If set-field values are incorrectly specified, the field value will not get updated when the ticket is saved.
- Modifications to an Auto-Route do not impact older records. They are applied next time the auto-route gets applied.

How Do I

Below are some actions you can take related to managing Auto-Routes.

Configure an Auto-Route

You can configure Auto-Routes for ticket to be routed to an identified Support Group or Support Technician based on ticket Matching Conditions. You can also configure actions that should get applied to the ticket when an auto-route gets applied to the ticket.

To access an Auto-Route record:

Step 1: Click on the Manage Auto-Routes link under Workflow Tools. A list of all Active Auto-Routes will be displayed in the table.

You can view and modify existing Auto-Routes and configure new Auto-Routes in this form.

To configure a new Auto-Route:

Step 2: Select a Ticket Type for which the Auto-Route will be applied. An Auto-Route can be related to only one ticket type.

Step 3: Enter a Name for the Auto-Route in the Name Field, which is a required field.

You can provide additional information in the Description field, though this is not a required field.

Step 4: Choose a Sort Order for the Auto-Route. You may choose not to set a Sort-Order, in which case, the Sort Order applied is 0.

Step 5: Click on Apply Changes to save the Auto-Route record.

The Auto-Workflow Action field now gets enabled. The Matching Conditions, Set Fields, Communications and Time tabs now get displayed on the Auto-Route record.

Step 6: If you want an action to get executed on the ticket when the Auto-Route is applied, you can choose a Workflow Action Option from the Workflow Action lookup.

Only those Action Option that are Active and applicable to the related ticket type will be listed in the lookup.

Step 7: In the Matching Conditions tab, you can configure Matching Conditions which will determine whether the Auto-Route gets applied or not.

You can configure multiple Matching Conditions for an Auto-Route.

Step 8: In the Set Fields tab, you can set field value for Assigned to Individual or Group which will control the Support Group or Individual to whom the ticket will get Auto-Routed.

Step 9: In the Set fields tab, you can configure other field values that will get set when the Auto-Route gets applied to the ticket.

Step 10: From the Communications tab, select communication templates that will be used to send out notifications when the Auto-Route is applied to a ticket.

You can choose multiple communication templates from the list.

Step 11: Configure a Schedule for an Auto-Route, which controls when the Auto-Route gets applied. If no schedule is configured, the Auto-Route gets applied 24X7.

Step 12: Click on Apply Change to save the schedule.

The Auto-Route will now get applied on all tickets with Matching Conditions defined on the Auto-Route. Execution of the Auto-Route will trigger the defined actions on the ticket.

Note:

If no Matching Conditions are set, the Auto-Route will get applied to all tickets of the related ticket type.

If a ticket conditions matches the Matching Condition of more than one Auto-Route, the Auto-Route with lowest Sort Order will get applied to the ticket.

Manage Matching Conditions

You can configure Matching Conditions for controlling applicability of an Action Option on a ticket at a particular stage, and for Auto-Routes applied for routing of new tickets.

The Matching Conditions tab gets enabled on an Action Option or Auto-Route after the record is saved.

To configure Matching Conditions:

Step 1: In the Matching Conditions form section, select Match Type as Include or Exclude from the dropdown list.

If the Match Type is INCLUDE, the Action Option/Auto-Route will get applied if the identified conditions exist on the ticket.

If the Match Type is EXCLUDE, the Action Option/Auto-Route will get applied if the identified conditions DO NOT EXIST on the ticket.

Step 2: Select a Sort Order for the Matching Condition statement.

Where more than one statement is configured as Matching Condition, the system will match for ALL identified conditions one after the other in the Sort Order indicated.

Step 3: Choose from the ticket field which you wish to use as Matching Condition; for example, Requester Organization/Source/Priority, etc.

Step 4 Below the field name, enter the value which should be matched for; for example, if the Field Name chosen as Matching Condition is Status, you can enter New/Pending/Active etc. in the field below.

You can configure one statement comprising of more than one field. For example, you can configure a statement which says "Status =Active OR New & Phase = Technical Approval & Reason Code = Submitted for Approval

Step 5: Click on Apply Changes to save the Matching Condition.

After one Matching Condition is saved, you can configure a second statement in the same way.

Matching Conditions can be configured using Standard Ticket Fields as well as Custom Fields on tickets. The fields Attribute 1 to Attribute 6 (with corresponding Attribute Value) let you set up Custom Fields as Matching Conditions.

You can also use the mailbox in which the mail was received and the Subject of the Email (which get logged as Ticket Description when the ticket is created) as Matching Conditions.

Note:

If not Matching Conditions are configured, the Action Option/Auto-Route gets applied to all tickets of the related ticket type.

You have to exercise due caution when entering field values as Matching Conditions. If an incorrect value (like a wrong spelling) is entered, the Action Option/Auto-Route will not get applied to any ticket.

Create a Schedule for Auto-Routes

You can configure a Schedule for an Auto-Route, which controls when the Auto-Route gets applied. For example, you may want a ticket to be routed to different support groups based on Support Group Schedules.

To configure a Schedule, locate the Auto-route record for which you wish to configure a Schedule.

If you wish to configure a Schedule for an existing Auto-Route, open the record from the Manage Auto-Route link under Workflow tools, locate the Auto-Route to which you wish to add a schedule and make required changes. The Time tab gets displayed on an Auto-Route record after it is first saved.

To configure a Schedule:

Step 1: Click on the Time tab of the Auto-Route.

Step 2: Enter the Start Date and End Date, Start Time and End Time for an Auto-Route.

Ideally, you can enter Start Time and End Time corresponding to the Support Group availability schedule.

Step 3: Select the Time-Zone which will be used to calculate Start and End Time/Date for the Schedule.

Step 4: Choose the days of the week during which the Auto-Route should be applied.

Step 5: Select a Holiday Group from the Holidays dropdown list.

If you want the Auto-Route to run only on Holidays in the Holiday Group, check the Runs only on Holidays checkbox.

Step 6: Click on Apply Changes to save the Schedule.

You can associate only one schedule for an auto-route.

Note: If no schedule is configured, the Auto-Route will be applied 24X7.

Configure Auto-Route or Workflow Action for Emails

You can configure Auto-Routes for new ticket to be routed to an identified support group based on the Email ID to which the ticket was sent. You can also configure Auto-Routing based on Subject of the Email.

To configure an Auto-Route based on Received in Mailbox field or Description field:

Step 1: Configure the Auto-Route as normal with Related Ticket Type and Auto Route Name.

Add description and Sort Order to the Auto-Route as appropriate.

Step 2: Click on Apply Changes to save the Auto-Route.

The Matching Conditions, Set Fields, Communication and Time tab now get enabled on the Auto-Route.

Step 3: Create the Matching Condition on the basis of which the Auto-Route should get applied.

In the Match Type say Include.

In the fields section below, where you can choose fields and values as Matching Conditions, there are two fields - Received in Mailbox and Description.

Step 4: To configure email ID as the Matching Condition; enter the Email ID to which the Email Request will be sent by the requester for that request.

Step 5 To configure Subject of the Email as Matching Condition, in the Description field enter Description as Matching Condition.

The requests from end users can thus be Auto-Routed by setting Matching Conditions as the Email ID to which the ticket is sent or the Ticket Description (the Subject of the Email sent by the requester).

Note: Multiple Email IDs can be configured for your Slice when your Slice is Provisioned. This is taken up by the Product Support Team. The Email ID used in Matching Condition must be configured for your Slice.

The Subject has to be an exact match for the Auto-Route to get applied. Spelling or other errors will mean that the Auto-Route will not get applied.

Subject or Sent to Mailbox can also be used as fields for configuring Workflow Action Options.

Frequently Asked Questions

This section lists questions and answers to common queries that users may encounter when working with Manage Auto-Routes in Nimsoft Service Desk.

Can the same auto-route be related to more than one ticket type?

No, an Auto-Route can be related to only one ticket type. The drop down list will not allow you to select more than one ticket type.

What does the sort order control in an auto-route?

The Sort Order of an Auto-Route controls the order in which the Auto-Route gets applied. While setting a sort order is not mandatory, it is good to set a high sort order for an Auto-Route with no matching conditions.

The Sort Order of an auto-route is particularly important when the ticket conditions match the Matching Conditions configured on more than one auto-route. In such a situation, the Auto-Route with the lower Sort Order will get applied to the ticket.

Can an Auto-route be created without specifying a Matching Condition? How could this affect the auto-route?

If you don't specify matching conditions for an Auto-Route, the Auto-Route will get applied by default to all tickets. Configuring Matching Conditions on an Auto-Route enables you to control what ticket the Auto-Route gets applied on.

What does the sort order control in the Auto Route?

The Sort Order of an Auto-Route controls the order in which the record will be displayed in the list of available Auto-Route.

The Sort Order of an Auto-Route becomes important when a ticket condition matches the condition of more than one Auto-Route. In such a condition, the Auto-Route with the lowest Sort Order gets applied.

What does the order of the Matching Condition SQL control?

The Order of the Matching Condition indicates the sequence in which the Matching Condition gets applied by the system. When a ticket is being matched for Matching Conditions of an Action Option, ALL Matching Conditions are matched one after another as per the Order indicated. You can change the Order without affecting the end result of the execution of the action.

You don't have to specify an order for the Matching Conditions. By default, the Order 0 gets applied.

How can two conditions be linked with "AND" operator?

Two conditions get linked with an AND operator when two or more Conditions are specified as EXCLUDE statements. For example, if you want to construct a matching condition where the Action Option should not get applied to a ticket if Status is New AND Priority is High AND Urgency is Critical

Two or more conditions also get linked with an AND Operator when One statement is INCLUDE statement and another statement is EXCLUDE Statement.

Can there be three or more conditions linked with "AND" operator or OR Operator?

Yes, you can configure Matching Conditions where three or more conditions are linked with AND Operators (Exclude Statement). You can also configure a Matching Condition where three or more statements are linked with OR Operator (Include Statements).

You can also configure matching conditions where some statements are linked with AND Operators; and some are linked with OR Operators. In such a condition, all the Include statements will be linked to the Exclude statements with an AND Operator.

Will adding new auto-routes impact existing tickets or will they only get applied to tickets created after the workflow action was configured?

An Auto-Route gets applied to a ticket only when the ticket is saved for the first time. Therefore, adding new Auto-Routes does not in any way impact older tickets. A new Auto-Route cannot get applied to existing tickets, as the existing ticket records would have already been saved and would have moved along their life-cycle.

What happens if I change the matching conditions or set-field values after an auto-route has already been applied?

Modification of the Set-Field values or matching conditions on an existing Auto-Route does not impact older records where the Auto-Route got applied in any way.

Modification impact only how the Auto-Route will function next time it gets applied to a ticket.

Can multiple communications get sent from the same auto-route?

Yes, you can associate more than one communication template with an auto-route and thus send out multiple notifications when an auto-route is applied to a ticket.

What happens if no information is filled in Time Tab for the Auto routing?

If no details are configured in the Time Tab of the Auto-Route, no schedule is associated with the Auto-Route. The Schedule of the Auto-Route controls when the auto-route is applied.

The default applicability of an Auto-Route is 24X7. Hence, if no schedule is configured, the Auto-Route gets applied round the clock.

What happens if only start Date is specified and end date is not specified?

In such a situation, the Schedule will be applied from the Date indicated in the Start Date and will be applicable perpetually after that date till the auto-route is active or otherwise modified.

Specifying Start and End Date controls the applicability duration of the Auto-Route.

What happens if both Start and End dates are not specified?

If no Start and End Dates are specified, the Auto-Route will get applied from the time it was configured and will continue to be applied to the tickets perpetually till the auto-route is active or otherwise modified.

What happens if more than one auto routing is found applicable to a ticket based on the Matching conditions?

If more than one Auto-Route is found applicable on the ticket, the Auto-Route with the lower Sort Order gets applied to the ticket.

What happens if a Service Desk Agent manually selects Assign to Individual before saving the ticket? Will the auto-route that should get applied work?

No, if the Service Desk Agent chooses to assign the Ticket using available Action Options before saving the ticket, the Auto-Route will not get applied on the ticket.

The manual action taken by the agent takes precedence over an auto-route.

Chapter 27- Manage Approval Groups

Overview

As IT related requests could have cost and performance related impacts, it becomes necessary to exercise control over processing requests for IT Services. This is particularly important when procuring a new IT object or service and bringing a change into the existing IT setup in the Organization.

A poorly planned or hastily implemented change could result in added costs and lost time and revenue. It is therefore essential that requests for change must be studied thoroughly, its implications must be understood clearly and the change should be approved by a competent authority.

Depending on the complexity and impact of the changes, you can configure either a simple approval process with a contextual approver like the Requester's Manager as Approver of the Change or define a change workflow process where the ticket moves through multiple levels of Approvals with action on Approval or Action on Rejection being defined.

In order to facilitate inclusion of an Approval process for change tickets, you can configure Approval Groups for different types of change tickets. Based on ticket matching conditions, the ticket could be sent to Approvers and Reviewers associated with the approval group.

Configuring Approval Groups eases the task of identifying approvers and reviewers for a particular type of change ticket.

An Approval Group can have named approvers i.e. contacts and support groups selected using the Name Search option and/or Contextual Approvers i.e. Contacts or Support Groups that get related from the context of a specific ticket, for example Requester's Manager, Change Approver of a CI related to the ticket etc.

This section deals with the activities associated with configuring Approvals and associated activities that need to be established for an Approval process to be accommodated.

Create or Modify Approval Groups

You can configure new Approval Groups and manage existing groups from the Manage Approval Groups link under Workflow Tools in the Navigation Menu. The Manage Approval Groups form contains a list of all existing Approval Groups. You can filter the list using the available filters or search for a specific group using the search option.

To view details of an existing Approval Group, click on an item in the list. The details will get populated in the form below. You can also configure new Approval Groups using this form.

The screenshot shows the 'Manage Approval Groups' form. It includes a table of existing approval groups and a detailed view of a selected group. The table lists groups like 'Approvals for Break-Fix change', 'Approvals for Normal Change', and 'Class Specific Approvals'. The details view for 'Approvals for Normal Change' shows fields for Ticket Type (Change Request), Name (Approvals for Normal Change), Description (Approvals for Normal Change), Status (Active), and Matching Criteria (Requesters Manager as an Approver, Requesters Manager as a Contextual Approver for Request, Financial Approver after CAB approval, Server Approver Reviewer Group, Service Provider Changes).

The main fields in the Manage Approval Groups form are listed below.

Field Name	Detailed Description
Ticket Type	This field displays the Ticket type to which the approval group is related. At present, approval is applicable only to Change Tickets. Hence, Change is the default ticket type; it is enabled in the read only format and cannot be changed.
Name	You can specify a name as the identifier for the Approval Group.
Description	You can provide a brief description about the approval group in this field.
Status	This field displays the current Status of the Approval Group. Deleting the group makes the status Inactive. You can set an Inactive record as active from this field.
Allow Agents to Modify List	You can allow the Service Desk Agent working on the ticket to modify the Approver list, if appropriate. If the value is set to yes, agents will be able to add or remove approvers when the ticket is being submitted for approval. The default value is NO.
Matching Criteria	You can configure Matching Conditions for the Approval Group using the logical operators and field name as appropriate.
Query	This field displays the Matching Condition configured for an approval group. You can add or remove field values and logical operators, as appropriate.

When a Change ticket is submitted for approval, based on the Matching Conditions on the ticket an Approval Group gets associated with the change ticket. The details of Approvers and Reviewers associated with the ticket get listed in the Approval tab of the ticket.

In this tab, all information regarding the Approval Phase, type and other related actions configured will be displayed.

If the action of Allow Agents to Modify List on Use is selected, the Service Desk Agent will be able to add Approvers or reviewer by manually adding or removing approvers/reviewers.

To move the ticket ahead in the Approval process, they can take an Approval related action (Submit for Approval) from the Take an Action Option on the ticket. The ticket will get submitted for approval. Notification regarding submission for approval or review gets sent to identified recipients. The system also sends out reminder Notifications for any pending approvals.

When you Create a new Approval Group, after the Approval Group record is saved, the Approvers and Reviewers tabs get enabled. You can now add Approvers and Reviewers to the Approval Group.

Add Approvers and Reviewers

You can add Approvers and Reviewers to an Approval Group to determine which Contact(s) and/or Support Group(s) will be related as Approvers or Reviewers of the Change Ticket where the Matching Conditions get applied.

You can choose to add either specific contacts or support groups as Approvers or Reviewers or choose for approvers to be added from the context of the ticket.

These Approver or Reviewer types are explained below:

Named Approvers or Reviewers

Named Approvers are those Contacts or Support Groups that are related to the Approval Group using the Name Search Lookup. You can select named Approvers by clicking the Add Approvers or Add Reviewers button in the Approvers or Reviewers tab respectively.

The Name Search lookup will be displayed. You can filter the list to view either Contacts or Support Groups and select the Contact(s) or Support Group(s) that you wish to add as Approvers.

Matching Criteria | Approvers | Reviewers

Add Contextual Approvers Add Approvers

Unrelate Approver Name

Unrelate Lombardino, James VPENG

Unrelate Tricom, Bill VPRT

Name Search

To find a Support Group. Refine your search using Group Name

View

Show Groups Contacts Groups

Group Name	Group ID	Description
Approval / Reviewer List	111	Contacts to be approvers/ reviewers in Approval Groups
BestTSM App Server Clusters Boston	60	BestTSM App Server Clusters Boston
BestTSM DB Mgt Boston	53	BestTSM DB Mgt Boston
BestTSM DB Server Cluster Baroda	63	BestTSM DB server Cluster Baroda
CAB	79	Change Advisory Board (CAB)
CAB-EC	81	Change Advisory Board - Emergency Committee (CAB-EC)

Record(s) 1 to 16 of 16

List of Approval Groups

Select Group/Contacts

Selected Contacts and Support Groups can be added as Approvers for a Change Ticket as part of an Approval Group. You can choose to add named approvers to an Approval Group based on organizational policies for approval.

For example, a contact who is Finance Manager (or a support group designated as Financial Advisors) could be selected as a Change Approver for an Approval Group that is required to approve all changes that have a specified financial cost associated with them.

When such a rule is in place, and the Contact or Support Group designated to approve such changes is known, you can select the name of that Contact or Support Group as Approver(s) for that Approval Group.

Note: Only Support Groups where the Used For Approvals flag is checked, and Contacts who are members of a Support Group where the Used for Approval flag is checked, can be added to an Approval Group as named approvers or reviewers

If you have allowed Agents to add approvers or reviewers when the Approval Group is applied to a ticket (by checking on the Allow Agents to Modify list on use checkbox), Agents can add other contacts as named approvers for the ticket.

Contextual Approvers or Reviewers

Contextual Approver or Reviewers are those contacts who become part of the change approval process based on the context of the ticket. Configuring Approval Groups with Contextual Approvers is an effective way of configuring an effective workflow for changes that do not need to go through an elaborate approval process.

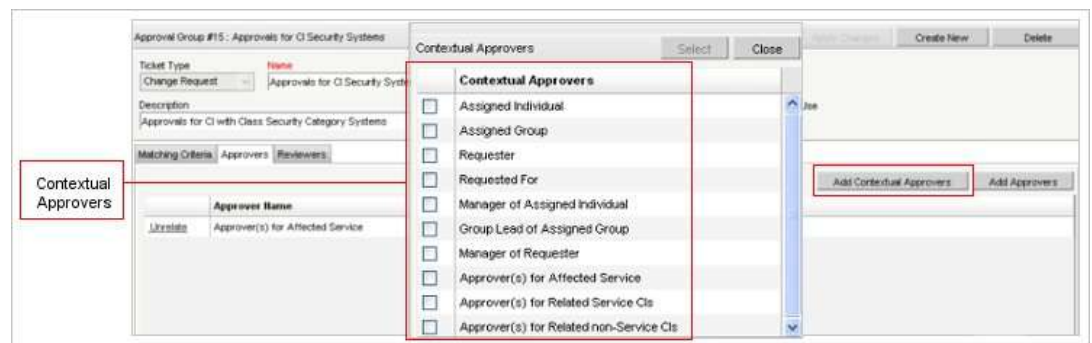
For example consider a Standard Change requesting upgrade of a system or software on an individual machine, or access to a training module for one user or group. While the process may require approval of the upgrade or training request, this change is unlikely to impact many users, or require major investigation.

For such request, you could configure a simple workflow, with the Manager or the Requester being the Change Approver.

Rather than having multiple Approval Groups (based on managers for the many organizational entities); you could choose a contextual approver to be identified based on the Requester of the ticket.

You can add Contextual Approvers and Reviewers from the Add Contextual Approver or Add Contextual Reviewer buttons in the Approvers and Reviewers tab respectively.

When you click on the Add Contextual Approvers or Add Contextual Reviewers tab, a Contextual Approvers/Reviewers lookup will be displayed with a list of available Contextual Approvers or Reviewers.



Check the checkbox indicating one or more Contextual Approvers/Reviewers and click Select to add the Contextual Approver/Reviewer to the Approval Group.

The Contextual Approvers or Contextual Reviewers that you can choose from are:

- Assigned Individual
- Assigned Group
- Requester
- Requested For
- Manager of Assigned Individual
- Group Lead of Assigned Group
- Manager of Requester
- Approver(s) or Reviewer(s) for Affected Services
- Approver(s) or Reviewer(s) for Related Service CIs

- Approver(s) or Reviewer(s) for Related Non-Service CIs

Depending on what type of Change request the approval group will get related to (based on Matching Conditions), you can select one or more appropriate contextual approvers

Contextual Approvers or Reviewers need not be members of Support Groups that are flagged as Used for Approvals. Any contact that has the appropriate relationship with the related record on the ticket can be a Contextual Approver or Reviewer.

Note: To fully exploit the feature of Contextual Approvers or Reviewers, you must provide required information on the relevant records, like set a Manager for a Contact in the Contact Record, choose a Group Lead for a Support Group in the Support Group record and Add contact(s) as Change Approver and Change Reviewer in the CI record.

Categorization Classes (CCTI) related to Configuration Items can be marked as 'Business Services' by adding it to the Config Parameter SLA_BUSINESS_SERVICES_IDENTIFIER. This demarcates Service CI and Non-Service CIs.

Agents working on the ticket cannot add Contextual Approvers or Reviewers to the ticket. They can only add named approvers or reviewers.

Approval Types

Change requests (other than standard, pre-approved changes) have to be approved. The proposed change is evaluated and submitted for approval to an Approval Group. Any user with login privileges can be a member of an Approval Group. An Approver can either approve or reject a ticket, or defer the decision and ask for more information.

As application administrator, you can set up workflow for a change approval process. A Work flow action can be used to submit a Ticket for Approval to an approval group. While configuring the workflow, you can choose Approval Type from one of the following options:

All Approvers: When this Approval Type is selected, ALL approvers must approve the ticket. If any approver (even one among all assigned approvers) rejects the ticket, the approval process ends and the change is rejected.

Any One Approver: A Change is approved as soon as any ONE approver approves. The change approval process does not wait for inputs from remaining approvers; the approval is rejected only when all approvers reject the proposal.

Any One Approve or Reject: A change is approved or rejected by a single approver from Approver Group. Thus, the decision of the first approver to "Approve" or "Reject" is applied to the Change request. In this case, the Approval process does not wait for inputs from the remaining approvers.

To configure a change approval process based on Approval Type, you can configure an auto-route to get applied by matching conditions to set fields for Approval Type. Subsequently, a workflow action can be configured to move the ticket through the approval process based on the Approval Type.

Approval Type option is available in Matching Conditions and Set Fields for Workflow actions and Auto-Routes.

Manage Approval Groups Check points

Some points to consider related to managing approval groups are:

- You can configure multiple approval groups for different approval related needs.
- Approval action is available only for Change Tickets.
- You can add Contextual Approvers/reviewers to an approval group, where the Approver/reviewer will be determined from the context of the ticket.
- To enable submitting change for approval, appropriate Action Options of Submit for Approval, Defer Change, Withdraw from approval, etc. must be configured.
- To enable notification of change submitted for approval; Communication Templates has to be available.
- You can set up multiple levels of approval and configure Workflow Actions to move the change from one approval stage to another.

How Do I

Below are some actions you can take related to Approval Groups.

Configure an Approval Group

You can configure Approval Groups which can be used when setting up workflow actions for Change Tickets. Approval Groups can be configured from the Manage Approval Groups under Workflow Tools in the Navigation Menu.

To access the form:

Step 1: Click on the Manage Approval Group link under Workflow Tools in the Navigation Menu.

A list of active Approval Groups will be displayed in the table. You can view and modify existing Approval Groups and configure new Approval Groups in the form below. Currently Approvals apply only to Change Tickets; hence Ticket Type is selected as Change by default.

To create a new Approval Group:

Step 2: Enter a Name for the Approval Group in the Name field, which is a required field.

You can add additional information in the description field, though this is not a required field.

Step 3: If you wish to allow Service Desk Agent working on the ticket to add or remove Approvers or Reviewers from Approval Group list when it gets applied to a tickets, click on Allow Agents to Modify List on Use radio button as Yes.

If set to yes, Service Desk Agents can make required modifications like choose fewer approvers based on the nature of the change or people availability etc. For more sensitive changes, you could set the value as No (which is the default setting).

Step 4: Configure the Matching Conditions based on which the Approval Group gets associated with the Change Ticket.

To configure the Matching Conditions, you have to use appropriate Logical Operators and choose relevant fields from the ticket to build the SQL query.

For example, you can specify Matching Criteria that when the Change Subtype is Normal; Approval Group A has to be applied. The SQL Query would be like this - ('\${change_subtype}'='Normal')

You can have more than one Matching Criteria for the Approval Group to get applied to the ticket. For example

('\${change_subtype}'='Break-Fix') AND '\${appr_phase}' != 'level_2_Financial'

Step 5: Click on Apply Changes to save the Approval Group.

Step 6: Click on the Approvers tab. In this tab you can choose to Add Contextual Approvers or Add Approvers.

When you choose to set Contextual Approvers like Requester's Manager, Requester, Requester's Group Lead etc.. the actual approver is picked based on who the requester of the ticket is.

You can also Add Approvers by choosing contacts from the Name Search Lookup. You can choose either Contacts or Support Groups as Approvers for the change.

Step 7: Relate Reviewers for the Change from the Add Reviewers tab.

Similar to Approvers, you can choose to Add Contextual Reviewers or Add Reviewers from the Name Search lookup.

You can unrelate Approvers or Reviewers as appropriate.

Note:

If no Matching Conditions are configured, the Approval Group will get applied to all Change Tickets.

If an illogical Matching Condition is configured, the Approval Group will not get applied to any Change Ticket.

Frequently Asked Questions

This section lists questions that you could have in configuring and managing Approval Groups. Click on a question to view the related response.

Is Approval related only to Change Tickets? Can I not configure an approval for other ticket types?

Currently, the functionality of Approvals is limited to only Change Tickets. At present you can configure Approval Groups and Approval based workflow actions only for Change Tickets within the application.

What does the field "Allow Agents to Modify List on Use" with the Radio-Button Yes/No indicate?

When Service Desk Agents work on a ticket, they can take an action of Submitting a ticket for Approval. Based on the matching conditions, an Approval Group gets associated with the ticket.

A list of approvers and reviewers who are related to the Approval Group get listed in the Approval Tab of the ticket.

If the Allow Agents to Modify List on Use is set as Yes, the Service Desk Agent will be able to remove approvers or reviewers from the list, and modify the list of Approvers who can Approve the request.

If the action is set as No, the Agent will not be able to remove approvers/reviewers from the list.

While allowing agents to modify the list is useful (or even desirable) for some standard requests, the decision to allow agents to modify the list of approvers or reviewers is up to you.

Do I have to set matching conditions before I select Approver or Reviewers?

There is no specific sequence in which you need to configure the Approval Group record. You can add approvers or reviewers before you configure matching conditions.

The Add Approvers and Add Reviewers action buttons get enabled once the Approval Group record is saved.

If you have saved the record before configuring Matching Conditions, you can choose the order in which you wish to configure the rest of the record.

Do I have to set matching conditions for an Approval Group? What is the implication of not setting Matching Conditions?

You can configure an Approval Group without setting any Matching Conditions. In such a situation, the Approval Group will get applied by default to all Change Tickets. The Approvers and Reviewers from that Approval Group will feature as Approvers/Reviewers for ALL changes.

Why do I see a Select action with some items in the Matching Conditions dropdown list (like ccti_id; while I see not such option with others (like appr_phase)?

The Matching Condition dropdown list displays a list of all fields available on a Ticket that is related to the record for which the Matching Conditions are being configured. This includes the standard Ticket Fields as well as Custom Fields that are applicable on a Change Ticket.

For example; if an Auto-Route is being configured for an Incident Ticket, all fields on an Incident Ticket will be listed, if an Approval Group record is being configured, all fields on a Change Ticket will be listed.

The Select Action, or a dropdown becomes available for all those fields where you can select values from a dropdown or lookup list on the Ticket Form (for example fields like Status, Priority, Categorize, etc).

Therefore, when configuring Matching Conditions, you see some fields where you need to specify text and others where you can choose from a dropdown list.

When configuring Matching Conditions, you must generally exercise caution to pick fields that can be used for valid Matching Conditions.

Which of the items in the Matching Conditions Dropdown list are best fit for Approval Groups?

Ideally, the fields suited for configuring Matching Conditions for Approval Group are ccti_id, status, phase, requester organization, change type, etc.

What do the fields Contextual Approvers/ Contextual Reviewers mean?

Contextual Approvers or Contextual Reviewers indicate that the name of the approver or reviewer will be selected from the context of the ticket.

For example, consider a Standard request for a Change (like access to some material or site on the internet), that does not need an elaborate Approval process. For such changes; you may require Approval from the Requester's manager.

If you configure an approval Group for such standard changes, you can select from the list of probable Contextual Approver or Contextual Reviewer. This includes people like Requester's Manager, Manager or Assigned Individual, Group Lead of the Requester, etc.

Based on the relevant information on the ticket (say requester name, or assigned to individual name), the contact who can approve the request will be identified by the system directly.

You can select Contextual Approver or Reviewer for standard requests where the approver or reviewers could change depending on factors like who has submitted the request.

Can I select multiple groups as Approver/Reviewer for the same Approval Group?

Yes, you can select multiple groups as Approver/Reviewer for an Approval Group. The Approver/Reviewer list associated with the Approval Group can also be a combination of Groups and individual contacts or just some members of a group (and not all).

You can unrelate members of the related Support Group that you do not want to make a part of the Approval Group.

Can agents add or remove approvers when they assign a ticket for approval?

Service Desk Agents can add or remove approvers from an approval group if the Allow Agents to Modify List on Use is set as Yes. Therefore, if you do not wish to allow modification of the Approval Group, you can set this field as No.

Can Agents view a list of approvers in an approval group?

Yes. Service Desk Agents can view a list of Approvers associated with a ticket in the Approvals Tab of the ticket.

Chapter 28 – Service Level Management

Overview

Service Level Management is the process of identifying the level of IT services needed to support a business organization's IT needs and designing a mechanism to ensure that the IT services are delivered as agreed upon.

Service Level Management also deals with defining a mechanism to monitor whether the identified service levels are being met or not.

Service Level Management involves setting up Service Level Agreement (SLA) to define what a service is and the level at which it must be provided. The Service Level Agreements also define the acceptable and unacceptable levels of service, liability on part of the service provider and the customer, and actions to be taken in specific circumstances.

Nimsoft Service Desk enables you to apply measurements to the Service Level Agreements in terms of time taken to respond to and resolve an issue. You can define the Service Targets based on available Service Metrics and set up Violation and Non-violation thresholds for measurement of service against agreed upon SLAs.

You can also set up actions such as Notifications or Escalation to be taken when a given SLA target is missed.

This section deals with the actions the Application Administrator can take to enable SLA Monitoring on Service Desk Tickets.

Service Metrics

Nimsoft Service Desk provides you a range of pre-defined Service Metrics that define what is to be measured. This includes parameters such as Response Time, Resolution Time, Holding Time, Closure time, etc.

You can create Service Targets based on the available Service metrics to quantify compliance measurements against a wide range of factors.

Manage Service Metrics

You can access Service Metrics from the Manage Service Metrics link under Service Level Management in the Navigation Menu . Clicking on this link displays the Manage Service Metrics form and the Service Metrics List. All Active Service Metrics are listed in the table. You can search for a specific Service Metrics by entering Service Metrics name or filter the list using available filters.

You cannot create new Service Metrics; also you can make only minor modifications to the available Service Metrics. This includes changes to the Metric name and description, or setting a Metric as Inactive.

The screenshot displays the 'Service Level Management (Manage Service Metrics)' window. On the left, there are three tabs: 'List Filters', 'Service Metrics List', and 'Service Metrics Details'. The 'Service Metrics List' tab is active, showing a table with the following data:

ID	Identifier	Metric Name	Description	Status
11	Response Time (Service A)	Response Time (Service A)	Service Level Metric used to monitor the response time to	Active
12	Request Holding Time for S	Request Holding Time for S	Service Level Metric used to monitor the response time to	Active
13	Request Holding Time for S	Request Holding Time for S	Service Level Metric used to monitor the response time to	Active
14	Response Time for Support	Response Time for Support	Service Level Metric used to monitor the response time to	Active

Below the list, the 'Service Metrics Details' tab is active, showing the details for 'Service Metric -15: Resolution Time (Service Availability H...'. The fields include:

- Ticket Type:** Change Request, Incident, Problem, Service Request, Task Ticket
- Identifier:** Resolution Time (Service Availability Hours)
- Metric Name:** Resolution Time (Service Availability Hours)
- Description:** Service Level Metric used to monitor the resolution time for tickets (time taken to provide a resolution for tickets) to track SLA compliance for an end-to-end business service that it impacts.
- Metric Calculation:** EXEC P_CALCULATE_SLA_RESOLUTION_TIME_METRICS @SLICE, @ITEM_ID, @METRIC_ID, 'Service'
- Status:** Active
- Metric Context:** Support Ticket, Support Group, Affected Service (all checked)
- Service Period:** Service Availability Hours

To view details of an existing Service Metric, click on an item in the list. The details get displayed in the Service Metrics form below. You can view details of the Service Metric. The main fields in the manage Service Metrics form are listed below.

Field Name	Detailed Description
Ticket Type	This field displays information on the ticket form to which the Service Metric is related.
Identifier	This field displays the unique name assigned to the Service Metric
Metric Name	By Default, this is the same name as the Identifier. However, you can modify this field to change the metric name as per your naming conventions.
Description	This field contains a brief description of the Service Metric giving more information about the metric. You can modify the description as required.
Metric Calculation	This field displays the SQL Query for the metric calculation
Status	This field displays the current status of the Service Metric. Deleting a Service Metric makes the status as Inactive.
Metric Context	This field provides information on the context which the metric is applied to. You can view the context applicable by seeing whether the checkbox in available options – i.e. Support Groups or Affected Services is checked or not.
Service Period	This field displays the basis of time period measurement for comparison with the target thresholds which the Service Metric considers. For Example 24X7 clock time or working hours of the Business Group to which the ticket is assigned or the Service Availability schedule for the Affected Services mentioned in the ticket being monitored.

There are a total of 21 pre-defined Service Metrics . The metrics are applied to measure Response Time, Response time by Status , Response Time by Support Groups , Resolution Time , Holding Time, and Closure Time

The main Service Metric, their description, the monitoring Start event and End event are explained below

Metric Name	Description	Start Event	End Event
Response Time (time for First Manual Action)	Time taken by a Service Desk Agent to manually acknowledge a ticket by taking an action on the ticket from the Take an Action option	Ticket creation time	Agent takes a manual action on the ticket from the Take An Action option. OR Ticket Status is changed to Resolved or Closed directly.
Response Time by Status (when status is set to Active)	Time taken to set the Ticket Status as Active for the first time since ticket creation. The status can be set as Active either through manual action or a pre-defined action by the system	Ticket creation time	Ticket is set to Active first time during the ticket life-cycle. OR Ticket Status is set to Resolved or Closed directly.
Resolution Time	Time taken to Resolve the ticket	Ticket creation time	Ticket Status is set to Resolved OR Ticket Status is directly set to Closed.
Closure Time	Time taken to Close a ticket	Ticket creation time	Ticket Status is set to Closed
Support Group Response Time	Time taken by a member of a Support Group to respond to a ticket assigned to the Support Group	Assignment to Group time	First manual action on the ticket by a member of the Support Group OR Ticket Status changes to Resolved or Closed
Request Holding Time for Support Group	Time duration for which a ticket was held by the Support Group in their	Assignment to Group time	Reassignment of the ticket to another Support

	queue		Group OR Ticket Status changes to Resolved or Closed.
Customer Communication Time	Time since the last communication was sent to the "Requested For" or the Last Client Viewable worklog on the ticket	Ticket Creation Time OR Last Communication to Requested For in 24X7 Support Environment	Communication sent to Requested for OR Client Viewable worklog entered OR Ticket status set to Resolved or Closed.

Each of the seven above ways of monitoring are applied to three methods of time measurement for elapsed time between Start Event and End Event; giving a total of 21 Service Metrics.

- 24X7- applied for continuous uninterrupted clock time.
- Support Group Business Hours - applied for working hours specified for the Assigned to Group.
- Service Availability Hours - applied when the Affected Services (for Configuration Items classified as Service) linked to the ticket being monitored is normally agreed upon to be available.

For example, consider a metric based on Group Business Hours: If Assigned Group for the ticket is scheduled to work from 8 AM to 4 PM, and a ticket is assigned to the group at 7 AM, The time measurement after Start Event (7AM) actually starts when the group is scheduled to be available (8 AM). If the Group responds to the ticket at 08.10 AM, then Response Time is 10 minutes and not 01 Hrs.10 minutes

You can choose to set a Service Metric Inactive; modify the Metric Name and Metric Description. You will not be able to make any other modifications to the Service Metrics.

Service Targets

Service Targets define the value at which an action on a ticket complies with existing agreements; or breaches the established service levels. Service Targets can be applied as measurement of compliance against a Service Level Agreement (SLA), Operational Level Agreement (OLA) or Underpinning Contract (UC).

Nimsoft Service Desk allows you to set Service Targets against the specific Service Metric to measure performance of a ticket against the Values measured by the Base Metric .

You can set up multiple Thresholds for a Service Target and specify one of the Thresholds as a Violation Threshold . You can also specify action to be taken when a threshold is violated.

This can include Notifications to identified stakeholders or Escalation of the ticket to another Support Groups .Nimsoft Service Desk allows for the ability to pause measured time calculations, if required.

While configuring a Service Target you can specify the status or statuses of tickets for which the measured time calculation has to be paused. Thus when a Service Target is applied to a ticket, the measured time calculation excludes the time spent by the ticket in the “Paused” status. The Due Date field is displayed as “To be determined”.

Manage Service Targets

You can access Service Targets from the Manage Service Targets link under Service Level Management in the Navigation Menu . Clicking on this link displays a list of Active Service Targets. You can filter the list using the available filters and search for a Service Targets by entering name in the search window.

% Service Level Management (Manage Service Targets)

Filter By: ☐ Agreement Type ☐ Status

ID	Ticket Type	Name	Description	Status
17	Service Request, Inci...	Resolution Time for TVPS Service Re...	Resolution Time for TVPS Service Request / Incident by External Su...	Active
18	Incident	Resolution time for TVPS incidents by...	Resolution Time for TVPS incidents by Internal Groups	Active
21	Incident	Response Time by Status	Response Time by Status	Active
22	Incident	Request Holding Time	Request Holding Time	Active
23	Incident	Ticket Closure Time	Tickets closure Time	Active
24	Change Request, Ser...	SRO Response Time Violation	SRO Response Time Violation	Active

Record(s) 1 to 9 of 9

Service Target #3: Default Request Response Rule

Name: Default Request Response Rule Status:

Base Metric: Response Time (24x7 Support) Paused Statuses:

Description: Default Request Management Metric for Response Time to Requests

Agreement Type: ☒ Service Level Agreement ☐ Operational Level Agreement ☐ Underpinning Contract

Matching Criteria: ☒ Threshold Rules ☐ Related Agreements

Applies To Ticket Type(s): Applies to Group(s): Applies to Service(s):

Matching Conditions:

Query:

When you click on an existing Service Target in the list, the details get displayed in the Service Targets form below. You can also create a new Service Targets from this form. The main fields in the Manage Service Targets form are listed below.

Field Name	Detailed Description
Name	You can specify a name as an Identifier for the Service Target
Base Metric	You can select a base Metric that will be applied to measure the elapsed time to which the Service Target threshold will be compared.
Description	In this field you can enter a brief explanation of what the target measures.
Paused Statuses	You can choose multiple ticket statuses from the lookup. The Measured Time calculations for the tickets in the chosen status will exclude time spent by the ticket in the Paused statuses
Agreement Type	These Radio Buttons allow you to set the Agreement Type as Service Level Agreement (SLA), Operating Level Agreement (OLA), or Underpinning Contract (UC).
Matching Criteria	This section allows you to define the criteria when the Service Target will get applied.
Applies to Ticket Type(s)	You can select which Ticket Type the Service Target gets applied to. A target can get applied to more than one ticket type.
Applies to Group(s)	You can choose which Support Group the Service Target is applied to.
Applies to Services(s)	If the Service Target is for a Service CI, you can choose the Service the target gets applied to from the lookup.
Matching Conditions	You can compose the Matching Conditions which will be matched for the Service Target to get applied to a ticket. You can choose the ticket conditions from the dropdown list and select appropriate values to compose the query.
Query	This field will display the matching conditions to select the ticket to which the service target will get applied.

You can configure Service Targets for different ticket types applied to different groups or the services as appropriate. The Service Targets get applied to the Base Service Metric to measure SLA compliance of the ticket.

Once the Service Target is configured, the Thresholds tab and Related Agreements tab get displayed. You can set up Threshold Values from the Threshold tab and if the current Service Target is related to any other targets, you can relate it from the Related Agreements tab.

Manage Thresholds

Threshold is the tolerance limit at which a pre-defined action sets off. You can specify multiple thresholds for a service target and designate one threshold as Violation Threshold. This means that at this Threshold; the SLA is being violated. You can also indicate what action is to be executed when a ticket violates a threshold.

The screenshot displays the 'Manage Thresholds' interface. At the top, a 'Threshold List' table shows a single rule. Below it, the 'Threshold Details' form allows for configuring a new rule, including logical operators, threshold values, actions, and notification templates.

Violation Threshold	Operator	Threshold	Action Name	Escalation to	Reminder	Notification Template	Sort Order
Yes	>=	5.0	Notification	Assigned Group	Send 1 Notifications	SLA Violation Notification	1

Record(s) 1 to 1 of 1

Apply Changes Create New Unrelate

Logical Operator: > Threshold Value (min.): 10.0 Action to Perform: Assignment Notification Template: [dropdown]

Contacts/Group related to Ticket: [dropdown] Other Contacts: [dropdown] Other Groups: [dropdown]

Manager of Assigned Individual: [dropdown]

Is Violation Threshold? ☒ Sort Order: 2 Reminder Frequency: [dropdown] Notifications every [] min.

The table displays a list of all Threshold Rules that are currently applied to the Service Target. You can add new Threshold Rules or remove a rule by unrelating it. The fields that allow you to manage threshold rules are listed below.

Field Name	Detailed Description
Logical Operators	You can choose a logical operator to specify the condition which will result in crossing of threshold limit. For example, when measured time becomes greater than (>) Threshold OR measured time equals the threshold or has become greater than (>=) the Threshold.
Threshold Value	You can specify the time (in minutes) at which the logical operator gets applied to for a Threshold Value.
Action to Perform	This field lets you define the action to be taken if the Threshold value is crossed. The possible actions you can specify are No Action, Email Notification, Phone Notification, or Escalation.
Notification Template	If you choose Email or Phone Notification as Action to Perform, this field gets enabled. You can choose a Notification Template to notify related recipients about the threshold violation.
Is Violation Threshold?	This checkbox lets you mark a threshold as a Violation Threshold. Only one threshold can be flagged as Violation Threshold. If only one threshold rule is configured, by default it is considered the violation threshold.
Sort Order	You can set a Sort Order to define which threshold rule takes precedence if more than one threshold rule has the same value.

Applies to Ticket Type(s)	You can select which Ticket Type the Service Target gets applied to. A target can get applied to more than one ticket type.
Applies to Group(s)	You can choose which Support Group the Service Target is applied to.
Applies to Services(s)	If the Service Target is for a Service CI, you can choose the Service the target gets applied to from the lookup.
Matching Conditions	You can compose the Matching Conditions which will be matched for the Service Target to get applied to a ticket. You can choose the ticket conditions from the dropdown list and select appropriate values to compose the query.
Query	This field will display the matching conditions to select the ticket to which the service target will get applied.
Reminder Frequency	If required, you can set a reminder frequency for a notification transmission against a threshold rule. The system will send out only one notification, or additional reminders for the same notification at specified intervals (till the metric calculation ends).

By setting up threshold rules for a Service Target, you can set up monitors for compliance for Service Level Agreements. For example, consider a Service Target to measure the Response Time to an Incident Ticket where Severity is High and Impact is High. The agreed upon Response time to such an incident could be 15 minutes.

You can set up three thresholds for this service target: one at 5 minutes; the second at 10 minutes; and the third at 15 minutes and earmark the third threshold as Violation Threshold. You can also specify action such as, if no one responds to the ticket in 15 minutes, a Notification is sent to identified contacts.

You can configure multiple Service Targets for different matching conditions on a ticket. For example, you can have a Service Target that gets applied to an Incident Ticket with Priority as Medium and another target for the same ticket when the priority as High.

If during the Ticket Life Cycle, the Service Desk Agent working on the ticket changes the ticket Priority from Medium to High, the service target for high priority with related matching conditions would get applied.

Similarly consider that ticket is assigned to a Support Group (say Level 1 support) which works 24X7. If service target for Response Time and Resolution Time for support group working 24X7 is configured, these Service Targets would get applied to the ticket.

However, if the ticket is then assigned to another group (say Level 2 support) which works at specified Business Hours, a different Service Target applicable to the support group Business Hours would get applied.

Thus, the Service Target gets monitored for compliance of threshold violation; and if violated, a pre-defined action is taken by the application.

Threshold Violation Actions

When configuring the Threshold Rules, you can specify what action is to be taken when a threshold value is reached. You can choose an available action from the 'Action to Perform' dropdown while configuring the Threshold Rules.

The screenshot displays the 'Actions' configuration window. At the top, there's a tabbed interface with 'Matching Criteria', 'Threshold Rules', and 'Related Agreements'. Below this is a table of threshold rules. The table has columns: Violation Threshold, Operator, Threshold, Action Name, Escalation to, Reminder, Notification Template, and Sort Order. The table shows three rows of data. Below the table, there's a 'Recent(s) 1 to 3 of 3' section. The main part of the window is a detailed configuration form for a selected rule. It includes fields for 'Logical Operator', 'Threshold Value', 'Action to Perform' (a dropdown menu with options: No Action, Assignment, Email Notification, Phone Notification), 'Notification Template', 'Other Groups', and 'Reminder Frequency'.

The options available are:

- No Action: When the Threshold value is reached, no action will get executed by the SLA monitor
- Assignment: When the Threshold value is reached, the ticket will get assigned to another group.
- Email Notification: When the Threshold value is reached, an Email Notification will be sent to the identified contacts/support group
- Phone Notification: When the Threshold value is reached, a Phone Notification* will be sent to identified contacts/support group

You can choose any One action to be performed per threshold rule. By setting an Action to Perform, you can enable to SLA Monitor to either notify contacts/support group about the threshold violation or escalate the ticket.

When configuring Support Groups (using the Manage Support Group form); you can set any Support Group to be the Next Escalation Group. You can use this configuration to move the ticket automatically to the next escalation group if a Threshold rule is violated. This will help ensure that defined Service Level Targets are met.

If you have subscribed for Phone Notification Service*, you can configure Phone Notifications to be sent out to related contacts or support groups when a Threshold is breached. The Phone Notification gets sent out using a Phone Notification Template (which you have to configure from the Manage Communication Template form).

A notification is sent out to identified recipients as an automated voice message, and the recipient(s) can choose from among pre-defined responses to the notification. The response in turn set off an associated workflow action, as configured under the External Notification tab of the Manage Configuration form.

Please note that for enabling SLA Phone Notifications, you will need to buy a license

from MIR3. Phone Notification is an external service provided by MIR3, and not a default feature available with Nimsoft Service Desk. Currently Phone Notifications are supported only for SLA Notifications, and not other notifications sent out by the application

Target Status

When SLA Compliance Monitoring is enabled on tickets, the SLA monitor scans for the Service Metrics and service targets that get applied to the ticket based on Matching Conditions.

When the matching conditions are met, the SLA monitor begins to monitor the ticket for SLA Compliance against the defined threshold rules.

Service Desk Agents working on the ticket can see the SLA Compliance Tab on the ticket. In this tab, they can view information on which Service Targets have been applied to the ticket. They can also view details on the Ticket Status, which indicates the status of the threshold of a Service Target that got applied to the ticket.

Some statuses get applied to Violation thresholds but not to non-violation thresholds. The explanation of the Target Status, what the status indicates, and whether it gets applied to Non-Violation thresholds or not is explained in the table below.

Target Status	Explanation	Applies to Non-Violation Threshold	Applies to Violation Threshold
In Progress	Threshold Condition has not been met. Service Metric Calculation is still in progress	Yes	Yes
Approaching Violation	Threshold Condition has not been met. Counter calculation indicates that a specified % of target value has been crossed	No	Yes
Met SLA	Violation Threshold has not been breached. Appropriate action on the ticket has been taken within specified threshold time specified	No	Yes
Missed SLA	Violation Threshold has been breached. Appropriate action has not been taken on the ticket within threshold time specified	No	Yes
Complete	Defined action has been executed and the Service Target has been met within Non-Violation Threshold	Yes	No
Aborted	Metric calculation stopped because the target became inapplicable before the End Event occurred. For example, the	Yes	Yes

	ticket got modified and so the matching condition was no longer met, so old Service Target is no longer applicable		
Ignored	When a Service Target gets applied due to changed matching conditions, any threshold conditions that have been satisfied but no action has been executed will be skipped; i.e. the earlier thresholds are ignored	Yes	Yes

Service Desk Agents can view the status of a Service Target and manage or prioritize their work on tickets accordingly.

Phone Notification Trace Logs

If your application administrator has undertaken the required configurations to enable the action of Phone Notification in response to an SLA Target Threshold rule violation, you can view the communication logs related to the status of the communication sent out from Nimsoft Service Desk and the response received from MIR3.

There are two background jobs that run to enable Nimsoft Service Desk to identify messages that need to be relayed to MIR3 and to relay the response from MIR 3 to those messages.

The table below shows the trace log messages generated in response to various scenarios of the SLA notification related messages exchanged between Nimsoft Service Desk and MIR 3.

Phone Notification Job	Message Text	Conditions in which the Trace Log Appears	Notification Status
Response Tracker	Notification Overridden by another action taken on the ticket	When an action is performed on the ticket before the recipient has responded to the phone notification	Notification Overridden
Response Tracker	Notification was Suppressed as the SLA Target that generated the Notification was Inactive	When the SLA Target is completed for the ticket as a result of the SLA getting missed or met	Suppressed
Response Tracker	Notification was responded. The selected response was: <<Textual Name of the option the recipient selected >>	When the recipient responds to a phone notification before the SLA getting missed	Notification Succeeded
Response Tracker	Notification has not been responded yet.	When a phone notification has been relayed to the recipient and the SLA is in progress	Delivered
Response Tracker	Notification has failed with Error Code: <<Response Code	Any MIR3 status other than RESPONDED for a phone	Notification Failed

	generated by MIR3 reflecting the status of the notification. >>	notification	
Relay Phone Notifications	Notification has Expired as the maximum expiration of <<Expiration Duration>> minutes was reached.	When a notification is not sent within a pre-defined timeout duration configured for the system. The default timeout is set to 15 mins. And CANNOT be modified by the service desk agent	Failed
Relay Phone Notifications	The phone notification was not sent because no recipients were specified in the To, CC or BCC list.	When the target recipient list for phone notification was empty or not available	Failed
Relay Phone Notifications	Notification is undeliverable. <u>An error log will also be generated as below:</u> An unexpected failure occurred when attempting to relay the phone notification via the third party notification system.	When an error occurs during relay of phone notification, and maximum retry attempts have been reached. The default retry attempts is set to 3 and CANNOT be modified by the service desk agent	Failed
Relay Phone Notifications	Notification could not be delivered. Delivery will be retried after some time.	When an error occurs during relay of phone notification and maximum retry attempts have NOT been reached. The default retry attempts is set at 3 and CANNOT be modified by the service desk agent	Delayed
Relay Phone Notifications	Notification is undeliverable. <u>An error log will also be generated as below:</u> An unexpected failure occurred while processing the notification for delivery.	When an unknown error occurs within Nimsoft Service Desk during the phone notification relay process	Failed
Relay Phone Notifications	Notification was suppressed as another action has already been taken on the ticket	When there is action taken on the ticket before the notification could actually be sent to MIR3 server	Suppressed
Relay Phone Notifications	Notification was suppressed as one of the previous notifications has already been responded to.	When any one of the previously relayed notifications for the currently applied SLA Target have already been responded to by the recipient	Suppressed
Relay Phone Notifications	Notification was suppressed as the SLA Target that generated Notification is inactive	When the SLA target does not apply anymore to the ticket and is therefore marked as met or	Suppressed

		missed	
Relay Phone Notification	The following recipients did not receive the notification since they are either marked as inactive or their phone number is not available <<list of recipients to whom notification was not delivered>>	When a phone notification could not be delivered to some recipients because of non-availability of their phone numbers or because they were inactive	Delivered

In case of notification failure, the trace logs can be used to identify the cause of failure.

Related Agreements

SLAs represent the customer facing agreements. To meet an SLA, operationally, participating support groups need targets at Group level. Targets for Support Groups of Internal service desk represent OLAs. Thus OLAs support SLAs.

If support is required from a Vendor (external Service Desk) with whom there is a contract (based on warranty or support agreement), these Underpinning contracts also support SLAs.

The Related Agreements Tab allows you to manage relationships between different Service Targets. From this tab, you can relate a service target to one or more existing service targets. You can also specify relationship type and specify if the current Service Targets supports the related target or is supported by the related agreement.

Relating agreements in this way allows you to view a more comprehensive picture of service targets applied to a ticket.

Manage SLA Monitoring

Organizations are increasingly using Service Level Agreements (SLAs) as a means to improve alignment of IT with business objectives, ensure predictable business performance, control costs and boost operational efficiencies. Given the need for IT Services and Support to meet agreed service level goals, applying SLA monitoring to tickets has become necessary.

However, not all organizations would want to impose SLA compliance monitoring on tickets. Nimsoft Service Desk allows you to choose whether or not to impose SLA monitoring and also allows you to manage SLA monitoring related aspects via the Slice Configuration Parameters.

Related Slice Parameters

You can choose whether you wish to enable SLA monitoring on tickets or not by setting Slice Configuration `ENABLE_SLA_MONITORING_ON_TICKETS` as Yes or No. If you choose to apply SLA monitoring on tickets by setting Parameter Value as Yes, Service Desk Agents will see the SLA Compliance Tab on the ticket.

This tab will display a list of all Service Targets that get applied to the ticket and the status of the ticket's performance against an SLA. They will be able to see if a ticket is approaching a Threshold violation, and the compliance status against a threshold (whether the ticket has met SLA, missed SLA, is approaching SLA violation, etc.) Agents can also filter the list using available filters. They can thus plan and prioritize their work towards meeting SLA targets.

If you choose to disable SLA monitoring, the SLA Compliance Tab will not be displayed on the ticket and none of the SLA related rules will get applied.

You can also manage other Slice parameters that define how the SLA monitoring function will get applied to tickets. You can filter the Slice Configurations by Parameter Category Service Level Agreement to view and manage these parameters.

Manage Service Targets Check points

Some points to keep in mind when managing SLA monitoring and management are:

- You can enable or disable SLA monitoring by setting an appropriate Slice Configuration Parameter Value.
- The SLA compliance Tab on tickets appears only when SLA monitoring is enabled.
- There are a fixed number of Service Metrics available. You cannot add or modify the Service Metrics.
- Multiple Service Targets can be configured with different Matching Conditions based on the same Service Metric.
- The Matching Conditions configured must be correctly configured for the Service Target to get applied.
- You can set multiple threshold rules for a Service Target. Any one threshold must be specified as Violation Threshold.

How Do I

Below are some actions you can take related to Managing SLAs.

Enable or Disable Service Level Monitoring

You can enable or disable SLA Monitoring on tickets by setting an appropriate value in the Slice Configuration Parameter `ENABLE_SLA_MONITORING_ON_TICKETS`.

To enable or disable SLA monitoring:

Step 1: Click on the Manage Slice Configuration link under Application Setup.

The Manage Slice Configuration form displays a list of all Slice Configurations that can be managed by you.

Step 2: Filter the list by Parameter Category. Clicking on Parameter Category displays a list of categories by which you can filter the list.

Step 3: From the Parameter Category list, choose Service Desk and click on Refresh to refresh the list.

All Parameters related to Service Desk will be listed.

Step 4: From the list, select Parameter `ENABLE_SLA_MONITORING_ON_TICKETS`.

Details of the parameter will be displayed in the form below.

Step 4: The Parameter Value field will display radio button options Yes and No.

Set the value option as Yes to enable SLA Monitoring or No to disable SLA Monitoring.

Note:

If SLA Monitoring is enabled, Service Desk Agents will be able to see the SLA Compliance tab on all tickets, and view details on Service Targets applied. If monitoring is disabled the tab will be hidden on all tickets.

Configure a Service Target against a Service Metric

You can configure a Service Target against a Service Metric from the Manage Service Targets link under Service Level Management. To configure a Service Target:

Step 1: Click on the Service Target link to view a list of all Active Service Targets. You can modify existing targets or create a new target in the form below.

To configure a new Service Target:

Step 2: Enter a Service Target Name in the Name field, which is a required field.

You can provide additional details in the Description field if necessary. However, this is not a required field, and you may choose to leave it blank.

Step 3: Choose a Base Metric against the Service Target is to be applied. You can choose from the available Service Metrics in the lookup. The lookup will display a list of all Active Service Metrics.

When you choose a Service Metric, the Related to Forms field in the Matching Condition section gets automatically updated with all forms that the Service Metric is related to. You can modify this list if required.

Step 4: In the Matching Conditions section, select which forms the Service Target will get applied to. The Lookup will display a list of forms the Service Metric is related to. Remove any form you wish to unrelate from the Service Target. You have to retain at least ONE form.

Step 5: If you want a Service Target to be applied specifically for some Support Groups, choose the Applies to Group from the Support Groups lookup.

If you want the Service Target to be applied to Services, you can select a Service from the Affected Services lookup.

Step 6: Construct the SQL query to configure the Matching Conditions for a Service Target. The Matching Conditions is to be constructed using appropriate field values from the dropdown list and relevant Logical Operators.

Step 7: Click on Apply Change to save the Service Target record.

When the Service Target is saved, additional tabs of Threshold Rules and Related Agreements are displayed on the form.

Step 8: In the Threshold Rules tab, Configure the Threshold values of the Service Target. You can configure more than one Threshold Value and specify any one as Violation Threshold.

Step 9: Set Actions to be taken when a Threshold is violated.

Step 10: From the Related Agreements tab, relate any other Service Targets to the newly configured Target.

You can choose not to Relate any Agreement to the newly configured Service Target. This will not impact how the Service Target gets applied.

Create Threshold Rules for a Service Target

You can configure Threshold Rules for a Service Target from the Threshold Rules tab of an existing Service Target.

To configure Threshold rules, open the Service Target for which you want to configure Threshold rules.

Step 1: Click on the Threshold Rules tab of the Service Target.

Any existing Threshold rules will be displayed in the list. Options to create new Threshold Rules are available in the form area below.

Step 2: To configure a new threshold rule, choose a logical operator from the dropdown list.

Step 3: In the Threshold Value field, specify time (in Minutes) as the target Threshold.

Step 4: In the Action to Perform field, select what action is to be executed if the Target Threshold is crossed.

You can choose to initiate no action, or choose the action of Notification or Escalation.

Step 5: If you choose action of Notification, the Notification Template field becomes a required field. Choose a Communication Template that will be used for notification about Threshold violation.

You can also set details on who is to be notified from the fields below.

Step 6: If you choose action of Assignment, you have to specify Contacts/Groups related to the ticket to whom the ticket gets assigned. You can also set Assignment to Other Contacts or Groups.

Step 7: You have to set a Sort Order for a Target Threshold. This defines the Order in which the Target gets applied.

Step 8: If the Target Threshold is a Violation Threshold (i.e. crossing this threshold signifies violation of the SLA) you can mark the threshold as Violation Threshold.

Note:

Ideally, the lower the Threshold time, the lower should be the Sort Order of a Target Threshold. For example if you want to apply Target Thresholds after every 15 minutes towards a Violation Threshold of 60 minutes, the first Target Threshold of 15 minutes should have Sort Order 0.

Configure Phone Notification for SLA Notification

You can configure Phone Notifications to be sent out when a Threshold value is reached on a Service Target. A Voice Notification gets sent out to identified recipients and based on the response to the notification, a related workflow action gets executed on the ticket.

Please note that for enabling SLA Phone Notifications, you will need to buy the service from MIR3. Phone Notification is an external service provided by MIR3, and not a default feature available with Nimsoft Service Desk. Currently Phone Notifications are supported only for SLA Notifications, and not other notifications sent out by the application.

If you have the required license from MIR 3 to enable Phone Notification, you will need to undertake configurations in the following forms to enable effective system whereby Phone Notifications can be delivered when a threshold rule value is reached, and configure the response to execute a workflow action.

- Manage Communication Templates- Enable Notification templates to be used for Phone Notifications
- Manage Service Targets- Setup meaningful Service Targets to get applied to tickets
- Manage Workflow Actions - Setup workflow actions to be executed in response to a phone notification
- Manage Configurations - Setup External Notifications tab with required information for enabling this service.
- Configure Job Triggers- Setup two triggers for running the relay and response tracker background jobs

To configure a communication template to be used for Phone Notifications:

Step 1: Click on the Manage Communication link under Workflow Tools. The Manage Communication Template form gets displayed.

You can either modify an existing template to use for SLA notification or configure a new template.

Step 2: In the Related to form field select Service Level Management to allow the communication template to be used for SLA notifications.

Step 3: Configure the To field to define who the notification should be sent to. You can select a recipient to be picked from the context of the ticket.

Step 4: Configure the subject and message body.

The Subject of the notification is consumed by MIR3, and the details in the Message Body are relayed to the recipients when the Phone Notification is relayed. To ensure message clarity, it is recommended that you keep the message body simple and easy to follow.

Step 5: In the Notification Method, select Phone to enable to communication template to be available for Phone Notifications.

Click on Apply Changes to save the communication template. This template will now become available when you configure a Threshold Rule Action under Manage Service Targets.

To exploit this functionality fully, you can provide contact details -Email ID and Phone Number- for the Support Group. This will allow communication to be sent to the common Support Group Phone number rather than individually send out communication to each member of a support group.

You can also configure the Next Escalation Group to define the escalation matrix for the support groups. This can be used for automatic escalation of the ticket if a SLA target is breached. These configurations need to be managed in the Manage Support Group form when setting up or modifying the Support Group records.

To Configure a Service Target with Phone Notification action:

Step 1: Click on Service Targets link under Service Level Management. The Service Targets form gets displayed.

You can either modify an existing Service Target or configure a new Service Target.

Step 2: Add in the required information, like Target Name and Base Metric. If you want the SLA calculations to be paused, you can set the status(es) at which the calculations must be paused.

Step 3: Set the Matching Conditions on the ticket which should be matched for the target to be applied.

Click Apply Changes to save the Service Target. The Threshold Rules tab and Related Agreements tab get displayed.

Step 4: In the Threshold Rules tab, Configure the Threshold rules. Select the logical Operator (Greater than or Greater than or Equal To) and set the threshold value time in minutes.

Step 5: In the Action to Perform field, select Phone Notification action.

The Notification Template field gets enabled and is displayed as Required field.

Step 6: Click on the notification template lookup. All communication templates which Active, Related to Service Level Management form and where Notification Method is Phone will be displayed.

Select a Communication template that should be used for sending out a Phone Notification.

Step 7: In the Contact/Groups related to the Ticket field; click on the lookup to view the Escalation to lookup. In this lookup, check on Next Escalation Group.

This will allow the ticket to be escalated to the group defined as the group to which the ticket should get escalated.

Step 8: Set the Sort Order for the threshold rule and apply changes to save the Service Target.

When this Service Target gets applied to a ticket, and if the ticket crosses the Threshold value defined, a Phone Notification will get sent to recipients defined in the Communication Template.

After setting up the Service Targets, you can proceed to configure workflow actions that can be executed by the system automatically based on the response received to a Phone Notification.

If you plan the Service Targets and Escalation Groups effectively, you can reduce the number of Service Targets configured and use the same target to be applied to multiple support groups rather than configure multiple Service Targets for monitoring similar threshold rules

While you can use workflow actions that you have previously configured; however, it is recommended that you configure Workflow Actions specifically to be used in response to Phone Notifications. This is because Workflow Action Matching Conditions and Required fields are ignored when the action is executed in response to Phone Notifications.

To configure workflow actions specific to SLA Phone Notification:

Step 1: Click on Manage Workflow Actions link under Workflow Tools.

The Manage Workflow Actions form will be displayed. You can modify an existing workflow action or configure a new workflow action.

Step 2: Enter the required field like Related to Form and Name for the Workflow Action.

You can choose a name that can be identified that allows you to identify the action as having been executed in response to an SLA Notification.

Do NOT associate any Special Function with the Workflow Action. If you associate a Special Function, the Workflow Action will not be available for Phone Notifications.

Step 3: Click Apply Changes to save the new Workflow Action.

The Matching Conditions, Set Fields, Required Fields, Communications and Permissions tab will get enabled on the form.

You can leave the Matching Conditions and Required Fields as blank. Any Matching Conditions and Required fields associated with the form will be ignored when the action is applied in response to a Phone Notification.

Step 4: In the Set Fields tab; set the ticket field values that need to be filled in when the Workflow Action is executed in response to a Phone Notification.

Step 5: In the communications tab, you can select any communication templates to specify any notifications that should get sent when the Workflow Action is executed.

As you are configuring these workflow actions to be available only for automatic action in response to a Phone Notification, you can choose not to assign permissions to the workflow action to any support group or role.

The Workflow Action is now configured and will be available for use for response to Automatic Notifications.

You can configure one Workflow Action to be used as Notification Failed Default Action. This is the default action which will get applied if a message notification from MIR3 to the intended recipients fails for any reason.

In addition to this, you can associate up to 5 workflow actions to be triggered when any one of the 5 corresponding Response to notification is selected by the recipient of the notification.

You can now configure the External Notification parameters to allow Phone Notifications and define the Response to Notification options.

To configure the Phone Notification:

Step 1: Click on the Manage Configurations link under Application Setup.

The Manage Configurations form will be displayed.

Step 2: Click on the External Notifications tab to view the form for configuring External Notifications.

Step 3: Check the Enable External Notifications Configuration checkbox. This will raise the flag that External Notifications are enabled and will allow the services to be setup and delivered.

When you subscribe to MIR3 for the Phone Notification service, you will be provided the User Name and Password as well as the URL from which Nimsoft Service Desk will connect with MIR3. You will need this information for configuring the system.

Step 4: In the System Name dropdown field; select MIR3.

Step 5: In the Username and Password fields, enter the User Name and Password provided by MIR 3 when you subscribed for the Phone Notification service.

Step 6: In the URL field, enter the URL provided by MIR3 (example:
<https://inwebservices.mir3.com/services/v1.2/mir3>)

You can now configure the Response to Notification section of the form.

Step 7: Click on the lookup for the Notification Failure Default Action field.

You can select the Workflow Action that you configured to be executed with the notification from MIR3 to the intended recipients fails.

Step 8: In the Response Options section, you can setup the Options that will be available to the recipients for actions they can take on the ticket when notified about the approaching SLA Threshold violation.

You can set up upto 5 response options and 5 corresponding Workflow Actions to be executed when any option is selected.

For example, if Response Option is I Acknowledge; an associated workflow action - Ticket Acknowledged can be set up.

Similarly for Response Option - I Escalate; an associated workflow action - Reassign to Group can be set up.

You can plan the workflow actions and Response Options based on what suits your organization best.

Step 9: Click on Apply Changes to save the configurations.

The configuration for SLA Phone Notification is now complete.

For Nimsoft Service Desk to process any queued Phone Notifications and for the application to process responses to these messages from MIR 3; there are two background jobs that need to be scheduled.

You can schedule these jobs from the Job Triggers tab in the Manage Configuration form.

To configure the Job Triggers:

Step 1: Click on the Job Triggers tab on the Manage Configurations form.

A list of all background jobs that are currently scheduled and enabled will be listed in the table.

Step 2: Click on Create New to schedule the new Job Triggers

The Configure Job Trigger window will be displayed.

Step 3: Provide a Trigger Name for the background job that lets you identify the Job Trigger.

Step 4: Click on the dropdown icon in the Job field.

A list of Background Jobs configured will be listed.

Step 5: From the dropdown list, select the Job Trigger 'Relay Phone Messages'

You can provide a trigger description if needed.

Step 6: In the Corn Expression field; set the frequency at which the background Job should run.

When configuring the frequency, ensure that the frequency of the background job is lesser than the lowest actionable target threshold value.

For example, if you have configured a Threshold Rule value as 10 minutes, and the action to be taken when that threshold value is reached is a Phone Notification; the Corn expression must be set a frequency of 2 or 3 minutes.

This is necessary to allow sufficient time for the background process to run and gather queued notifications and deliver them to MIR3; and for the response from MIR 3 to be collected and relayed back to the application in time.

Step 7: Set the Priority for the Corn Expression by choosing an option from the dropdown.

Step 8: Select the Time-Zone for the Job to run.

Step 9: Click on Apply Changes to save the Job Trigger.

You can follow the same process for the second job trigger 'Track and Monitor Message Responses'.

Once the background jobs are configured; all required configurations for enabling the SLA Phone notification feature are complete

Frequently Asked Questions

This section lists questions you may encounter when applying Service Level Management.

Can I create SLA targets for all ticket types?

Yes, you can configure SLA targets for all types of tickets. However, discretion is advisable on which ticket types you configure SLA targets. Some ticket types, like Problem or Change Tickets could have a very long resolution time with a long life-cycle making them unlikely candidates for SLA monitoring.

Can I create new Service Metrics or modify a Service Metric?

You cannot create a new Service Metric. You can only configure Service Targets against available Service Metrics.

You can make some modifications like changing the Metric name or metric description. You can also set a Service Metric as Inactive or make an Inactive metric as Active.

Can the same Service Target be applied to multiple ticket types?

Yes; a Service Target can be applied to multiple ticket types. The Relate to Ticket Type lookup allows you to choose multiple ticket forms.

Do I have to select an Applies to Ticket Type(s) field?

Yes, you have to select at least one ticket type to which a Service Target gets applied. By default all ticket types are selected in this field. You will not be able to save the changes unless you select at least one Ticket Type.

What happens if I configure a Service Target but do not set any matching conditions?

If no Matching Conditions are configured, the Service Target gets applied to all ticket types and Groups and/or Services that have been specified in the Service Target.

How many threshold values can a Service Target have?

You can configure multiple Threshold values for a Service Target. There is no specified limit. You can determine how many thresholds you wish to configure.

Please note that only one of the Threshold values can be marked as Violation Threshold.

What sort of actions can I configure if an SLA threshold is violated?

You can configure action of Notification to identified contacts or Escalation of the ticket to identified individual or group when it is violated.

You can also decide that no action is to be taken in case a threshold is crossed for non-violation threshold.

Can I modify a threshold value after it is saved?

No, once a threshold value is saved, it cannot be modified. You can unrelate the threshold and create a new threshold.

What does the Sort Order of a Threshold indicate?

The Sort order of a Threshold indicates the order in which a target threshold gets applied. A Threshold target with a lower Sort Order gets applied first, followed by a threshold of higher sort order.

Can I disable SLA Monitoring after having used in for some time? How does it impact tickets where SLA targets have already been applied?

You can disable SLA monitoring after it has been applied. The SLA monitoring will continue on the tickets where it has already been applied and the monitoring will exit gracefully after completing monitoring.

SLA monitoring will not get applied on tickets created after SLA monitoring was disabled.

How do agents know whether SLA is being monitored or not?

If SLA monitoring is enabled on tickets, the tickets will display a SLA Compliance Tab. In this tab the agents will be able to view information on SLA targets that have been applied to the ticket and the threshold status.

If SLA monitoring is disabled, the SLA compliance tab will be hidden and hence no information on SLA will be applied or displayed.

Chapter 29 – Service Feedback

Overview

Monitoring performance quantitatively and qualitatively is essential for continuous improvement. While monitoring for SLA Compliance provides a means of quantitatively monitoring performance, Service Feedback is a method of getting the End Users' opinion about the quality of services received for IT Services and Support.

The Service Feedback Module of Nimsoft Service Desk enables you to set up a Service Feedback mechanism to survey Service Desk functioning. You can create Service Feedback Surveys and set a Schedule for the Surveys to be sent to identified contacts and Support Groups as per a specified Schedule .

The Service Feedback Surveys can be made up of multiple choice responses or single line or multi-line text responses. A list of surveys can be configured and used as per need with different Service Feedback Schedules.

The schedule can be configured to solicit Anonymous Feedback without reference to the respondent or be configured to reflect respondent name. You can also specify schedule repetition patterns.

Once a schedule is associated with a Service Feedback form, the survey will get initialized as per the Schedule Respondents can see the survey form in the My Feedback Link in the application. They also receive email Notifications for the survey and can respond to the survey by accessing the survey from the link.

All actions related to managing the Service Feedback Module are explained in this section.

Manage Feedback Forms

To send out service feedback surveys, the first action is creating the Surveys with the required questions and appropriate answer formats. The Manage Feedback Form enables you to design a new Service Feedback Questionnaire with questions and appropriate response options using features such as Radio buttons, Check Boxes, or single/multi line text.

A feedback form can be made up of different question types. You can set up:

- Single option Multiple Choice Questions (radio buttons) with up to five possible responses

- Multiple options multiple choice questions (check boxes) with up to five possible responses
- Single Line free text response
- Multi line free text response

All new feedback forms are in Draft State and can be modified. A form in draft status can also be deleted permanently. A feedback form in Draft State cannot be related to a Feedback Schedule.

Once a feedback form is published, it can be associated with a Schedule. The published form cannot be modified or deleted.

Accessing Feedback Forms

You can access feedback forms from the Manage Feedback Forms link under Service Feedback Module. Clicking on this link displays a list of existing feedback forms.

You can search for a specific survey form by entering appropriate search text in the search window.

You can view details about a Service Feedback Form by clicking on the form name in the list. The related details are displayed in the form below. All new Service Feedback Forms remain in Draft State. In this status, the form can be modified. Once satisfied with the modifications, you can set the status as Published.

Once published, the form cannot be edited, modified, or deleted. You can only preview the form to view the survey questionnaire.

Create Feedback Forms

You can create new feedback forms for use as Surveys. To create a new Service Feedback form, you can specify a feedback form name; provide a description (not mandatory); and associate a Communication Template which will be used to send out Notifications of the survey.

You have to associate a Communication Template with the feedback form. You can choose from the available Communication Templates in the Dropdown List. Email notification about the Schedule will be sent to the recipients and they will be able to access the survey from the direct URL link in the Notifications.

Once the form is saved, you can add questions to the form; specifying the response type; and possible value options, if appropriate. . You can also manage the sequence in which the questions will appear by specifying Sequence Number for the question.

You can delete a feedback form that is in Draft Status. Deleting the form will result in the form being removed permanently.

History Tab

The History Tab of the Feedback Form contains data on the usage of the form in a schedule (schedule name), number of participants, respondents, and active till details. A consolidated history of all feedback schedules can be accessed from the Review Feedback Results forms.

Manage Feedback Schedules

To be effective a Service Feedback Survey should be sent to identified respondents at a specific interval. Also, you may want to send out Anonymous Feedback forms where the respondents can submit a response without providing user name. This helps the Service Feedback process become more transparent.

Nimsoft Service Desk allows you to manage both Anonymous and Non-Anonymous Service Feedback Schedules.

If the Schedule is anonymous, the user name will not appear on the feedback form. An Anonymous Feedback can also be set to allow duplicate responses.

You can configure a Service Feedback Schedule to fire a Feedback form at a specified interval. This interval could either be

- Number of days elapsed since last feedback
- Number of tickets logged by the respondent.

If the schedule is meant to be fired only once without any repeat pattern, you can choose 'No Repeat' in the options available.

Access Feedback Schedules

You can access feedback schedules from the Manage Feedback Schedules link in the Service Feedback Module. Clicking on this link displays a list of all available Feedback Schedules. You can search for a specific schedule by entering relevant details in the search window.

When you click on an entry in the Feedback Schedules list, the details of the Schedule get populated in the form below.

The screenshot displays the 'Service Feedbacks (Manage Feedback Schedules)' interface. At the top, there is a search bar. Below it is a table with the following columns: ID, Schedule Name, Schedule Description, Form Name, Participants, and Status. The table contains one record with ID 2, Schedule Name 'Schedule Initiated', Schedule Description 'Schedule 1', Form Name 'Customer Satisfaction', Participants 'Admin, Boston, Arrow, Alfre...', and Status 'Completed'. Below the table, there is a section for 'Service Feedback Schedule' details. This section includes fields for 'Schedule Name', 'Schedule Description', 'Service Feedback Form Name', 'Participant' (with a dropdown for 'Names'), 'Organizations' (with a dropdown), and 'Status' (set to 'Not Initiated'). There are also checkboxes for 'Anonymous Feedback Only' and 'Allow Duplicate Responses'. The 'Recurrence Pattern' section has two tabs: 'Recurrence Pattern' and 'Messaging'. Under 'Recurrence Pattern', there are fields for 'Starts On' and 'Ends On', and a 'Repeat' section with three radio button options: 'Every' (number of tickets counting, Any Tickets, Service Request, Incidents, Problems, Changes, Tasks), 'Every' (number of days), and 'No Repeat' (selected). There is also an 'Active For' field (number of days from the day the feedback is requested from end user). The 'Notification' section has a dropdown for 'Notify to Contact on Feedback Responses'.

You cannot edit or in any way modify or delete a schedule that has been initiated, completed, or aborted. You can modify a Schedule where the Status is 'Not-Initiated'.

This schedule can be modified or deleted. However, once initiated; you can only abort the schedule or allow it to run towards completion. All Schedules, including ones that are 'Completed' continue to be listed in the Schedules list above.

Create Feedback Schedule

You can create a new Feedback Schedule using this form. To create a new Feedback Schedule, specify a Schedule Name and choose a Service Feedback Form. A lookup with the available Feedback Forms will be displayed.

Service Feedback Form

Feedback ID: Form Name:

User Name:

Initiated On:

Active Till:

1. Open Request list ease of use
☐ Poor ☐ Acceptable ☐ Good ☐ Very Good ☐ Excellent

2. Open Request List > Issue faced in use or Suggestion for Improvement

3. Request Catalog Ease of Use
☐ Poor ☐ Acceptable ☐ Good ☐ Very Good ☐ Excellent

4. Request Catalog > Issue faced in use or Sugegstion for Improvement

5. Request Catalog > Frequency of Use
☐ Never ☐ Rarely ☐ Half of the time ☐ Most of the time ☐ Always

Service Feedback Form Detail

You can select the form you wish to associate and relate it to the schedule. You can also choose to make a schedule Anonymous and if made Anonymous, you can also decide if multiple responses are to be allowed or not.

A feedback scheduled can be sent to Contacts, Groups, or Organizations. You can choose from the Dropdown List as appropriate. Depending on the Participant Option, an appropriate lookup will be displayed to choose participants. You can choose multiple participants for a schedule.

Feedback Schedule Recurrence Pattern

Having determined the participants, you can set the Start Date (and if required, the End Date) for the Schedule. You can set a Recurrence Pattern for the Schedule; this will define if the schedule is repeated per number of tickets or per days.

If number of tickets is chosen, you can specify which ticket type(s) are to be considered as well. You can also set a schedule to be fired only once i.e. No Repeat.

Messaging Tab

In the Messaging tab, you can type out Notifications messages to be displayed if a user tries to access a Survey that has been aborted; that is inactive; or if a response has already been submitted (where duplicate response is not allowed).

You can also choose contact(s) to whom Notifications of response to the survey is to be forwarded. This will result in all responses to the surveys being forwarded to an appropriate contact for example a Service Delivery Manager.

Review Feedback Results

Once a Service Feedback Survey has been scheduled; you can view progress of the schedule in the Review Feedback Results form. Clicking on the Review Feedback Results link displays a table containing the status of all Feedback Schedules that have been initiated.

You can view data on Feedback Form and schedule used, participant and respondent details, Schedule dates, etc. This form provides a consolidated list for all feedback schedules that have been initiated.

This allows you to visualize the progress of a Feedback Schedule and take required follow up actions.

Service Feedback Reports

Nimsoft Service Desk provides an out-of-the-box report on Service Feedback responses. This report gives a summary of feedback responses received against each question in the feedback form.

For questions that allow respondents to select one or more options (Radio Buttons or Check Boxes), you can view the data as percentage statistics for each possible response value.

For questions where respondents are able to give text feedback (single line or multi line), in addition to simple statistics of Percentage Responded versus Percentage Not Responded, you can choose to view the actual responses by each respondent.

You can also choose to include charts in the report. The charts can be seen on screen or can be extracted as a PDF or CSV file.

As application administrator, you can manage access to these reports for Service Desk Agents or any other role responsible for customer satisfaction or continuous improvement.

Administering Service Feedback

As Application Administrator, you can manage the ability of contacts to participate in the service feedback process, manage access to the Service Feedback Module for Service Desk Agents (or a role focused on managing customer response and satisfaction), configure service feedback forms; and manage feedback schedules.

The actions related to managing access to Service Feedback and participation in Service Feedback are explained below.

Enable or Disable Service Feedback

You can manage the ability of contacts to participate in the service feedback process by checking or unchecking the Disable Service Feedback option on the Contact Record. When the Disable Service Feedback option is checked, the contact will not receive a Service Feedback Survey and will not be able to respond to the survey.

The ability of respondents to participate in Service Feedback is controlled at the Organization Level or Support Groups level as well as at the contact level. A contact will not receive Service Feedback Notification if:

- Primary Organization is Excluded from Service Feedback
- Primary Group is Excluded from Service Feedback
- Contact is Excluded from Service Feedback

If the Disable Service Feedback is checked for the Organization, no contact related to that organization (as Primary Organization) will be able to receive and respond to the Service Feedback Surveys.

Similarly, if the Disable Service Feedback is checked at the Support Group level, all contacts who are part of that Group (as Primary Group) will receive Service Feedback Schedules.

The Disable Service Feedback has to be unchecked at all levels (Primary Organization, Primary Group and Contact) for a contact to receive and respond to Service Feedback surveys.

My Feedback Link

Participants in the Service Feedback Process receive email notification when a feedback schedule is initiated. They can access the feedback survey by clicking on the link in the email.

Participants also view a schedule from the My Feedback link in the Navigation Menu. As Application Administrator, you can enable or disable access to this link by managing permission for access to this link.

Self-Service Users see the My Feedback link under Home section; while Service Desk Agents view this link under Service Feedback Section in the Navigation Menu.

When access to this link is enabled, the participant can see a list of feedback schedules that are active. The participant can click on an item in the list to view the survey form below, and respond to the Survey from the application interface. A schedule remains listed in the My Feedback list till the schedule is active or it is aborted.

Service Feedbacks (My Feedbacks)

Filter By: Status

ID	Scheduled Name	Feedback Form Name	Date Notified to User	Due By	Status
1860	SCH for Anonymous (Anonymous)	Customer Satisfaction	27/01/2011 04:30...		Pending

Record(s) 1 to 1 of 1

Service Feedback Form: Customer Satisfaction Submit

Feedback ID: 1874 **Form Name:** Customer Satisfaction

User Name: Anonymous, User

Initiated On: 16/03/2011 03:09:43 AM

Active Till:

1. Politeness/Empathy with which complaint was handled
☐ Excellent ☐ Good ☐ Satisfactory ☐ Can be better
2. Quality of initial response
☐ Excellent ☐ Good ☐ Satisfactory ☐ Can be better
3. Professionalism of the Service Desk Agent
☐ Excellent ☐ Good ☐ Satisfactory ☐ Can be better
4. Initial call response made by the Service Desk Agent in accordance with the agreed Call Service Level Agreement (SLA):
☐ Yes ☐ No

For an Anonymous schedule, the user name will not be listed in the User Name section of the survey form.

Also, in an anonymous service feedback, participants can view a schedule even after they have submitted a response; if a schedule does not permit duplicate responses, the form will open in Read Only mode. The participant will not be able to modify or resubmit the form.

Manage Service Feedback Check Points

Some key features of Service Feedback and points to remember when managing Service Feedback are listed below.

- The Disable Service Feedback flag controls whether a contact can participate in Service Feedback process or not.
- Access to the My Feedback link is managed by permissions. You have to assign permission for a contact to see the link.
- A Service Feedback Form cannot be modified or deleted after it is Published.
- A Feedback Schedule can be set to seek Anonymous Feedback.

- Anonymous schedules can be configured to allow duplicate responses.
- Once initiated, a Feedback Schedule cannot be modified or deleted.
- A feedback schedule can be aborted before it is complete.

How Do I

Below are some actions you can take related to Service Feedbacks.

Create a Service Feedback Survey Form

You can configure Service Feedback Surveys from the Manage Feedback Form link under Service Feedback. To create a new Service Feedback Survey:

Step 1: Click on the Manage Service Feedback form under Service Feedback module.

A list of all existing feedback surveys will be displayed. You can view details of an existing survey or create a new Survey in the form below.

Step 2: Enter a Name in the Feedback form Name field, which is a required field.

You can add additional information in the Description field if needed. However, you can choose to leave it blank as this is not mandatory.

Step 3: Select a Notification Template that will be used to notify respondents about the Survey executed. You can pick only one template from the list.

The Notification Templates lookup will display only those Communication Templates that are related to Service Feedback Forms.

Step 4: Click on Apply Changes to save the Service Feedback Form.

The Form tab and History Tab will now be displayed on the form. By default the status of the Feedback Form will be set as Draft. You can now add questions to the form.

To configure questions to be displayed in the feedback form:

Step 5: Select a Sequence for the question, which is a required field.

Step 6: Type in the Question in the Question field, which is a required field. This field accepts free text. You can frame a question as appropriate to the form.

Step 7: Select a Question Type from the dropdown list.

You can choose from multiple choice questions (Radio Button or Checkboxes) or free text response (single line or multi-line text).

Step 8: If the Question Type is Checkboxes or Radio Button, enter the options that the respondent can choose from.

You will be prompted to provide at least TWO options when you choose a multiple choice question type.

Step 9: Click on Save to save the question.

The question will get listed in the table above. You can add as many questions as required to the Survey form.

To remove a question from the Survey, select the question you wish to remove. The details will get displayed in the Question form below. Click on Delete, and the question will get removed permanently.

Once satisfied with the questions included in the survey, you can preview the survey form.

Step 10: Click on Preview action button to see how the questions are laid out, and if appropriate responses have been added or not.

If you are fully satisfied with the Survey form, you can change the status to Published.

Step 11: To set Status as Published, click on the Published radio button in the Status section of the form and click on Apply Changes.

You will get a message notifying the Published survey forms cannot be modified. You can continue to save the form if you are satisfied with the form.

Once the Survey form is Published, you will not be able to make any changes to it. You cannot even delete a feedback form after it is published.

Only Published Survey forms can be used when configuring a Service Feedback Schedule.

Manage Service Feedback Schedule

You can configure Service Feedback Surveys from the Manage Feedback Form link under Service Feedback. To create a new Service Feedback Survey:

Step 1: Click on the Manage Service Feedback form under Service Feedback module.

A list of all existing feedback surveys will be displayed. You can view details of an existing survey or create a new Survey in the form below.

Step 2: Enter a Name in the Feedback form Name field, which is a required field.

You can add additional information in the Description field if needed. However, you can choose to leave it blank as this is not mandatory.

Step 3: Select a Notification Template that will be used to notify respondents about the Survey executed. You can pick only one template from the list.

The Notification Templates lookup will display only those Communication Templates that are related to Service Feedback Forms.

Step 4: Click on Apply Changes to save the Service Feedback Form.

The Form tab and History Tab will now be displayed on the form. By default the status of the Feedback Form will be set as Draft. You can now add questions to the form.

To configure questions to be displayed in the feedback form:

Step 5: Select a Sequence for the question, which is a required field.

Step 6: Type in the Question in the Question field, which is a required field. This field accepts free text. You can frame a question as appropriate to the form.

Step 7: Select a Question Type from the dropdown list.

You can choose from multiple choice questions (Radio Button or Checkboxes) or free text response (single line or multi-line text).

Step 8: If the Question Type is Checkboxes or Radio Button, enter the options that the respondent can choose from.

You will be prompted to provide at least TWO options when you choose a multiple choice question type.

Step 9: Click on Save to save the question.

The question will get listed in the table above. You can add as many questions as required to the Survey form.

To remove a question from the Survey, select the question you wish to remove. The details will get displayed in the Question form below. Click on Delete, and the question will get removed permanently.

Once satisfied with the questions included in the survey, you can preview the survey form.

Step 10: Click on Preview action button to see how the questions are laid out, and if appropriate responses have been added or not.

If you are fully satisfied with the Survey form, you can change the status to Published.

Step 11: To set Status as Published, click on the Published radio button in the Status section of the form and click on Apply Changes.

You will get a message notifying the Published survey forms cannot be modified. You can continue to save the form if you are satisfied with the form.

Once the Survey form is Published, you will not be able to make any changes to it. You cannot even delete a feedback form after it is published.

Only Published Survey forms can be used when configuring a Service Feedback Schedule.

Monitor and Assist Respondents

You can monitor progress of a Service Feedback Schedule from the Review Feedback Results link in the Service Feedback Module. You can also extract a report based on completed Schedules to view responses and take actions on feedback responses.

You can assist respondents on how to respond to a Service Feedback Schedule.

Service Desk Agents and Administrators can access Service Feedback forms from the My Feedback link in the Service Feedback Module of the application. Self-Service Users access Service Feedback from the My Feedback link under Home.

To respond to the Service Feedback survey:

Step 1: Click on the My Feedback link under Service Feedback or Home as applicable.

A list of all active schedules will be listed in the table. The user can view the Status of the Schedule, as well as schedule Start Date and End Date.

Step 2: Click on a Survey you wish to respond to. The details will be displayed in the form below.

Step 3: Enter your feedback as appropriate, and click on Submit.

The feedback will get submitted. The status will change as appropriate. However, the Schedule will continue to be listed til it Expires or the schedule is Aborted.

If the Service Feedback Schedule is configured as Anonymous and allows duplicate responses; users will be able to submit response to a feedback Form more than once.

Frequently Asked Questions

This section answers some questions you could have related to Managing Service Feedbacks.

What type of questions can I include in a Service Feedback Form?

The question types you can use are:

- Single Option Multiple Choice Questions with up to 5 options (radio buttons)
- Multiple Option Multiple Choice Questions (checkboxes)
- Single Line text responses
- Multi-line text responses

Can I modify a Service Feedback Form after it is created and in use?

You can modify a Service Feedback form that is in Draft status. Once a Service Feedback form is Published, you will not be able to modify it.

When you initiate action to set a Service Feedback form as Published, you will get a message notifying you that once you change the Status to Published, you will not be able to make changes to it.

Can multiple schedules be associated to the same service feedback form?

Yes, you can use the same Service Feedback form for multiple schedules. The same form can be used simultaneously for different Service Feedback Schedules. There is no restriction on how often a form is used.

What information/details will be maintained in the History Tab of a Feedback Form?

The History tab of the feedback form displays information on the Service Feedback Schedules the form is associated with and the status of the Service Feedback Schedules where the form is used.

Which Notification templates are displayed in the Notification Templates Look-up list on a Service Feedback form?

All communication templates that are related to Service Feedback form will be listed in the Notification template lookup that is associated with a feedback form.

Can I associate multiple notification templates to a Service Feedback Form?

No, you can attach only one communication templates to a Service Feedback form. The lookup will allow you to search from all available Communication Templates related to Service Feedback form; however, only one form can be related.

Can recipients of a Feedback form submit their feedback without logging into the application?

Yes, respondents can submit their feedback without logging in to the application. The Service Feedback Schedule notification contains a Direct URL link which takes the respondents directly to the Survey form which respondents can fill in and submit.

Can I configure a feedback to be submitted anonymously?

Yes, you can configure a Service Feedback Schedule as Anonymous schedule. By configuring a Schedule as Anonymous, you can allow respondents to submit feedback anonymously.

Why are organizations or groups not displayed in the search form when selecting recipients of a Service Feedback Schedule?

The Name Search Lookup displayed for associating respondents to a Service Feedback Schedule displays only those Organization, Support Groups, or Contacts who can participate in the Service Feedback process.

This is controlled by checking or unchecking the Disable Service Feedback checkbox for the Organization, Support Group, and Contact.

Can I change the messages to be displayed (in the messaging tab) after a schedule is initiated? What is the possible impact of such a change?

Yes, you can change the message displayed in the Messaging tab of a Schedule. This will not impact the schedule in any way as the message gets displayed when the condition on the message gets applicable.

What happens if I specify only a start date for a schedule and no end date?

You can choose to specify only start date and not an end date for a schedule. However, you will need to choose a recurrence pattern for the schedule with no end date.

If you don't specify an end date for the schedule, the system will prompt you to specify either end date or Active for days or some other recurrence pattern.

What is the function of the field Notify to Contact on Feedback Responses?

The Notify to Contact field on Manage Feedback Schedule form allows you to direct responses to a Service Feedback Survey from the respondents of that schedule.

In this field, you can choose the contact to whom all responses from that Schedule should get redirected to. When respondents submit their response, the completed survey form gets sent to the email id of the identified contact.

How can I keep track of progress on a Service Feedback Schedule?

You can keep track of the progress of a Service Feedback schedule from the Review Service Feedback link.

This link displays details about the number of respondents for a survey, how many participants have responded, etc.

Will agents be able to access Service Feedback related report?

You can enable access to the Service Feedback related report for contacts designated as Service Desk Agents by giving permissions to the Service Feedback related report to the contact, support group, or role.

Can I create a new report specific to the service feedback needs of my organization?

You can use the Service Feedback report key to create a new report for Service Feedback. However, you will not be able to configure a unique report key specific to your needs.

Chapter 30 – Manage Schedules

Overview

Service Desk Agents who work at the IT Support or Service Desk, handle requests from the end-users which are assigned to them in the form or tickets. Much of the work done is reactive in nature as the need for IT support cannot be cleanly predicted.

However; there are some tasks that Service Desk Agents would be required to take on as part of routine maintenance of the IT Objects and devices. This could be tasks such as taking data backups, monitoring logs, preparing reports, or other such tasks that form part of the Service Desk tasks.

For such tasks which are regular and usually done on a fixed date and often at a fixed time, Nimsoft Service Desk allows configuration of Schedules.

As Application Administrator, you can configure a schedule for each such tasks. The system will generate a ticket as per the schedule specifications and the tickets will get assigned to the schedule owner.

Configuring schedules takes away the need to maintain a separate calendar for routine tasks and ensures routine tasks are assigned and tracked via tickets.

Manage Schedules

You can configure and manage schedules from the Manage Schedules link under Workflow Tools in the Navigation Menu. Clicking on this link displays the Manage Schedules form and the Schedules List tab. All Active schedules are listed in the tab.

You can search for a specific schedule by entering schedule name. When you click on an existing schedule in the list, the details get displayed in the Schedule Details tab. You can also create a new schedule in this tab.

Workflow Tools (Manage Schedules)

Manage Schedules

Schedule List | Schedule Details | Log

Schedule #2: Review of Failed attempts to access...

Apply Changes | Create New | Cancel

Schedule Details

Schedule Owner: Bakeman, Bo EN021 | Name: Review of Failed attempts to access Design Data | Status: Inactive

Description: Review of Failed attempts to access Design Data

Setting Schedule

Execute At (HH): 09:00 | Time Zone: (GMT-05:00) America/New_York | Holiday List: USA 2010 Over

Start Date: 01/05/2010 | End Date: | or End After: 3 | Recurrences: Every

Recurrence: Weekly | 1 | Week(s) On: Sunday ☐ Monday ☒ Tuesday ☒ Wednesday ☐ Thursday ☒ Friday ☐ Saturday ☐ All Days

Action on Schedule

Schedule Action: Create Ticket using Template

Ticket Template Name: Review of Failed attempts to access Design Data

☐ Override Auto Route

The main fields in the manage schedule form are listed below.

Field Name	Detailed Description
Schedule Owner	This is a required field where you can specify who owns the schedule. The tickets created get assigned to the Schedule owner.
Name	This is a required field and is used to specify a schedule name as its identifier.
Status	You can view current Status of the schedule. Deleting the schedule makes the status inactive. You can set status as Active from this field.
Description	This field can be used to provide brief details about the schedule and add any information.
Execute At	You can set a the time-zone for the schedule and the schedule will get executed at the specified time as per the Time Zone .
Holiday List	A schedule can be configured to exclude holidays in the Holiday List.
Dates	You can specify a start date for the schedule (required field) and an end date, if the schedule is for a fixed duration.
Ends After	A schedule can also be configured to be executed for a fixed number of times by specifying a number in this field.
Recurrence	A schedule can be set to be daily, weekly, monthly, or yearly by setting appropriate values in this field.
Ticket Template	You can specify the template that is to be used for creation of the ticket by choosing from available templates. Task Templates will not be available for creating tickets for schedules.

	Only Service Request, Incident , Problem , or Change Ticket Templates will be available in the lookup.
Override Auto-Route	If the ticket is to be assigned to the owner to prevent any other Auto-Route getting applied, you have to override Auto-Route

A schedule can be created for activities to be done by an identified individual. This reduces the effort needed by the Schedule Owner to repeatedly create tickets for a fixed routine activity. It also takes away the need to manage a calendar for routine activities separately.

The Integration Engine creates a ticket, as per the specified execution time and Recurrence Pattern , using the Ticket Template associated with the schedule. The ticket gets assigned by the routing engine to the schedule owner at the scheduled date and time.

The ticket details are pre-populated as per on the Set Fields specified in the Ticket Template. However, if the Override Auto-Route checkbox is not checked, any Auto-Route that matches the ticket Matching Conditions will get applied.

The ticket will get assigned to a support group as per the Matching Conditions of the Auto-Route; and will not get assigned to the Schedule Owner. Thus without manual intervention, you can manage routine activities using Schedules.

The maximum number of Schedules that can be in Active Status and be run at one time is controlled by the Configuration Parameter MAX_ACTIVE_SCHEDULED_TASKS.

Schedule Log

The Schedule log tab displays details about an Active Schedule. This tab contains information about a schedule owner, schedule details, action taken, and information on whether the schedule was successfully executed or it failed.

The column containing the Trace Log gives Additional Information about why the schedule is in the specified status. This helps in investigation and resolution if a schedule fails.

Workflow Tools (Manage Schedules)

Manage Schedules

Schedule List | Schedule Details | Log

Search

LogID	Schedule Owner	Schedule Name	Schedule Action	Case#	Executed On	Status	Trace Log
1	Dalglish, Sam ITS11	Weekly Back Ups for ERP	Create Ticket Using Template	313-215	31/05/2010 02:58:40 PM	Succeeded	Service Request with CASE#313-21 was created and assigned to Dalglish Sam ITS11
2	Cardoni, Julia	US Firewall log Review by BestSM Networking	Create Ticket Using Template	314-216	31/05/2010 02:58:40 PM	Succeeded	Service Request with CASE#314-21 was created and assigned to ,
3	Databases, Support Executive	Database Abnormal Activity review for ERP and Design Database	Create Ticket Using Template	318-217	01/06/2010 07:30:12 PM	Succeeded	Service Request with CASE#318-21 was created and assigned to Databases, Support Executive
4	Cardoni, Julia	US Firewall log Review by BestSM Networking	Create Ticket Using Template	320-218	02/06/2010 05:30:12 PM	Succeeded	Service Request with CASE#320-21 was created and assigned to ,
5	Cardoni, Julia	US Firewall log Review by BestSM Networking	Create Ticket Using Template	323-219	04/06/2010 05:30:12 PM	Succeeded	Service Request with CASE#323-21 was created and assigned to ,
6	Dalglish, Sam ITS11	Weekly Back Ups for ERP	Create Ticket Using Template	324-220	05/06/2010 01:30:12 AM	Succeeded	Service Request with CASE#324-22 was created and assigned to Dalglish Sam ITS11
7	Cardoni, Julia	US Firewall log Review by BestSM Networking	Create Ticket Using Template	333-223	07/06/2010 05:30:14 PM	Succeeded	Service Request with CASE#333-22 was created and assigned to ,
8	Bakeman, Bo EN021	Review of Failed attempts to access Design Data	Create Ticket Using Template	334-224	07/06/2010 06:30:13 PM	Succeeded	Service Request with CASE#334-22 was created and assigned to Bakeman Bo EN021
9	Cardoni, Julia	US Firewall log Review by BestSM Networking	Create Ticket Using Template	337-227	09/06/2010 05:30:14 PM	Succeeded	Service Request with CASE#337-22 was created and assigned to ,
10	Cardoni, Julia	US Firewall log Review by BestSM Networking	Create Ticket Using Template	338-228	11/06/2010 05:30:19 PM	Succeeded	Service Request with CASE#338-22 was created and assigned to ,

Schedule Log

You can view details of the Schedule Log on screen; or extract the data into a PDF or CSV file.

Manage Schedule Check points

Some points to note while managing Schedules are:

- A schedule has a specified Owner. The ticket gets assigned to the Schedule Owner; not the Support Group.
- You can control assignment of the Schedule by checking or not checking the Override Auto-Route checkbox.
- The Recurrence Pattern controls when the schedule ticket gets fired; hence this should be fixed with care.
- If a Holiday List is associated, the schedule will not get applied during the holidays identified.
- Only a fixed number of Schedules can be Active at a time, as managed by the Configuration Parameter.

How Do I

Below are some actions you can take related to Schedules.

Create a Schedule for routine Service Desk Activities

You can configure a schedule for routine Service Desk activities from the Manage Schedule link under Workflow Tools. To Configure a Schedule:

Step 1: Click on the Manage Schedule link under Workflow Tools. The List of active schedules will be displayed.

Step 2: Click on the Create New action button.

A blank Manage Schedules form will be displayed in the Schedule Details tab. The Schedule Owner field will display the name of the logged in user who is creating the schedule.

Step 3: Select a Schedule Owner and Schedule Name as appropriate. The Name Search Lookup will be displayed with you click on the lookup. You can select a Schedule Owner from this lookup. You can type in a Schedule name for the Schedule in the Name field.

You can add a description if required.

Step 4: Fill in execution related details like Execute At (time) and Start Date for the Schedule. This manages when the schedule will get initiated, and at what time (per the recurrence pattern) the schedule will get executed.

You can specify a Time-Zone at which the Schedule is to be executed. If no time zone is selected; it will default to the Schedule Owner's Time Zone. You can also attach a Holiday List to the Schedule if required.

Step 5: Set the Recurrence Pattern for the Schedule. You have to set either an end date for the schedule or a recurrence pattern.

You can choose a recurrence pattern as weekly, monthly or yearly. You can specify how often in the recurrence pattern the schedule will get executed.

Step 6: You can choose the Ticket Template which is to be used for creating the ticket for the Schedule. You can check on the Override Auto-Route Checkbox to avoid application of an auto-route to the ticket created for the schedule.

A ticket will get created using the ticket template attached, and will get assigned to the Schedule Owner as per the recurrence pattern set.

You can also modify a Schedule after it has been configured. The modifications will get applied the next time the Schedule is initiated.

Note:

A Schedule can be used only to create Service, Incident, Problem and Change Tickets. The Ticket Template Look up will not display Task Templates.

You have to check the Override Auto-Route checkbox to ensure that the ticket gets routed to the Schedule Owner. If this checkbox is not checked, the ticket can get routed to a different support group if some other auto-route gets applied based on the set field values of the ticket template.

You can control the maximum number of active schedule by setting the appropriate values in the Slice Configuration MAX_ACTIVE_SCHEDULED_TASKS. The default value is 50.

Frequently Asked Questions

Below are answers to some questions you may have related to managing Schedules.

Can one schedule have more than one Schedule Owner?

No; you can specify only one individual as Schedule Owner for a Schedule.

Will agents know that tickets being assigned to them are part of a schedule?

All tickets for a schedule are created automatically by the Integration Engine. This will be displayed in the Created By field in the Ticket Details section of the ticket.

Agents can see this field to confirm if a ticket assigned is part of a schedule.

Can agents create a schedule for their own routine work?

Configuring a Schedule is an administrative action, available as part of the Admin Modules.

If you wish to delegate this task, you can configure a support group or role to take on this task and assign permissions to the Manage Schedule link in the Navigation Menu for the support group or role.

Contacts associated with that support group or role can then configure and manage Schedule tickets for routine activities.

Can I know whether a schedule was successful or not?

Yes, you can view the status of a schedule to see whether it was successful or not.

The Schedule Log tab displays all information about the status and execution details of the Schedule. You can also view the Trace Logs to see why a Schedule failed.

What happens if I set only a start date for a Schedule and do not provide an end date?

If you select only a Start date for the schedule and no end date, the Schedule will get applied perpetually as per the specified recurrence pattern.

You have to specify either the end date for the Schedule or specify a recurrence pattern. If neither end date nor recurrence pattern is specified, the schedule will not get saved.

Do I have to set a recurrence pattern for a schedule? What will happen if I do not set a recurrence pattern?

You can choose to not set a recurrence pattern for a schedule. If you select the recurrence pattern as None, the fields that prompt you to select recurrence pattern get hidden.

However, you will have to specify the end date for the schedule if you choose not to set a recurrence pattern. In the absence of both, you will not be able to create the Schedule.

Will auto-routes get applied to a ticket created by a Schedule as well?

Yes; auto-routes will get applied to a ticket created by a schedule if the ticket meets the matching conditions of an auto-route. You can avoid auto-routing of the schedule ticket by checking the Override Auto-Route checkbox.

Can a schedule owner be changed after the schedule is already in place?

Yes, you can modify a schedule to change the schedule owner even on an existing active schedule. When such a change is made, the ticket created by the Schedule after the change is made gets assigned to the newly identified Schedule Owner.

What happens if I modify a ticket template that is being used for a schedule?

The modified ticket template will be used to create the ticket the next time the schedule is due to be executed. No impact will be seen on older tickets that have been created using the template.

Chapter 31 – Manage Defined Searches

Overview

In routine operations, Service Desk Agents working on ticket may feel the need for searching for specific type of records. Service Desk Agents have access to defined search and advanced search options.

The Advanced Search functionality available on the Agent Interface allows agents to specify a search parameter using one or more fields from the form the search is related to. If more than one field is specified, the search engine will extract data which matches ALL parameters specified.

When using Advanced Search, the search criteria has to be specified each time the search is executed.

The Defined Search functionality enables you to construct a search query for more specific search needs; and save the query to be executed whenever needed. Based on queries frequently used by Service Desk Agents, you can configure an SQL query to include or exclude specific data elements and search for data most relevant in the context of the search.

Defining Searches reduces the efforts needed by Agents to pull out data from the system and enables them to access appropriate data when needed. As the output is designed to be more specific, the effort of sorting through unwanted data is reduced.

As Application Administrator, you can create new Defined Searches , and manage access to all available Defined Searches via permissions.

Manage Defined Searches

You can manage and create new Defined Searches from the Manage Defined Searches link under Workflow Tools in the Navigation Menu. Clicking on this link displays a list of available Defined Searches. You can filter the list using available filter options. To view more details about an existing defined search, click on an item in the list. The Defined Search details get populated in the form below.

Workflow Tools (Manage Defined Searches)

Filter By: Form Name Category Name Type Search

ID	Related To Form	Category Name	Search Name	Help Text	Sort Order
2	Home, Service Request	Default	My Group's Open Service R...	My Group's Open Service Requests	2
3	Home, Service Request	Default	Tickets Not Assigned to Any...	Tickets Not Assigned to Any Group or Individual	3
4	Home, Service Request	Default	Service Request Updated wi...	Service Request Updated within last 7 Days	4
5	Home, Service Request	Default	Open Service Request Not U...	Open Service Request Not Updated within La...	5
6	Home, Service Request	Default	Open Service Request Appr...	Open Service Request Approaching SLA Viol...	6
7	Home, Service Request	Default	Open Service Request Violat...	Open Service Request Violating SLAs	7

View 1 - 20 of 61

Defined Search #29: All Scheduled Approved Change Req...

Apply Changes Create New Delete

Related To Form: Home, Change Request Search Name: All Scheduled Approved Change Requests Category Name: Default

Help Text: All scheduled change requests that have been approved and awaiting implementation.

Sort Order: 0

Query Permissions

Source: VAPP_CHANGE

Select List: CAST(case_id AS VARCHAR)~'+CAST(ticket_id AS VARCHAR) AS Case#, ticket_type AS 'Ticket Type', created_date AS 'Created Date', ticket_status AS Status, ticket_description AS 'Symptom Description', ticket_search_code AS 'Search Code' (assigned to last name + ' + assigned to name) AS 'Action In

Search Condition: APPROVAL_STATUS='Approved'

No Match Message

Field Data To Use

You can modify an existing defined search or manage permissions to the existing defined search. You can also use the form to configure a new defined search. The main fields in the Manage Defined Search Form are listed below.

Field Name	Detailed Description
Related To Form	You can relate a Defined Search to multiple forms in the lookup. Only Data related to these forms can be queried using this defined search.
Search Name	You can specify a name for the Defined Search as its identifier.
Category Name	You categorize the Defined Search as per your preference. All out-of-box Defined Searches are categorized as Default. You can create a new category name for any defined search that you configure
Sort Order	The sort order indicates the order in which the Defined Search will be listed in the Pre-Defined Searches page.
Help Text	You can provide a brief description for the defined search, to provide information about the data being queried.
Query	This tab allows you to manage the Defined Search SQL Query.

SQL Operators	The listed standard SQL Operators can be used to build the Search Criteria.
Source	You can select the Database view or table on which the search will operate from this field.
Select List	The full details of record(s) that the search condition pulls out of the Database are not included in the Search result display. You have to manually configure a select list of variables to include those fields with their value in search result display.
Search Condition	You can specify the Search Conditions or variables and their values for the "Where" condition of the Search. The fields from the form can be used as place markers for this field.
No Match Message	You can specify a message to be displayed if there are no records matching the search conditions. You can use field from the related form as place markers on the message.
Preview Result	You can use this to preview the search result. If the query is incorrect, an appropriate message will be displayed.
Field Data To Use	You can access Fields from the GUI for the related forms, which can be used as place markers, if needed, in Search Condition and No Match Message fields.
Permission	You can manage access to the defined search by managing Permissions to users, Support Groups, and Roles.

A variety of pre-configured searches are available as system Defined Searches. You cannot make any modifications to these pre-configured queries or delete these queries. You can, however; enable or disable access to these searches for contacts, Support Groups, and roles.

All other non-system defined searches can be deleted and permanently removed from the instance.

Manage Defined Searches Check Points

Some points to keep in mind when managing Defined Searches are:

- A defined search can be related to more than one ticket form and/or to Configuration Items.
- You can configure an SQL query to search the data from the appropriate source in the database.

- You have to manually enter a Select List to specify what data is to be gathered and how it is to be displayed.
- Where field data is used to specify Search Condition, the data has to match with records in the database.
- If the SQL query is incorrectly configured, an error message will be displayed asking you to submit a relevant query.
- You cannot modify system defined search queries.
- Deleting a defined search results in the record being permanently removed.

How Do I

Below are some actions you can take related to Defined Searches.

Configure a Defined Search

You can Configure a Defined Search from the Manage Defined Search link under Workflow Tools. To Configure a Defined Search:

Step 1: Click on the Manage Defined Search Link to view the Manage Defined Search form. A list of active defined searches will be displayed in the table.

You can modify an existing defined search or create a new defined search in the form below.

To create a new defined search:

Step 2: Relate forms to the defined search in the Related to Form field. You can relate a defined search to multiple forms by choosing more than one form from the Related Forms lookup.

Step 3: Enter a Name for the defined search in the Name field, which is a required field.

You can provide additional information in the Help Text field if needed; and specify a Sort Order for the defined Search. However, these fields are not required fields. You can leave them blank.

Defined Searches draw out data from your instance of the application based on the SQL query that is constructed. The steps to construct the SQL query and configure the search are listed below.

Step 4: Select the source that will be used to draw out data from the database. You can select the source from the dropdown list.

Step 5: In the Select List field, construct the SQL Query. To construct the query, you have to use appropriate logical operators and database field names. In the Select list, you can configure the data elements to be queried in the selected source and how the data is to be grouped and listed.

Step 6: In the Search Conditions field; you can construct the SQL query that defines the "Where" condition of the search. You can insert fields from the form that the search is related to for constructing this query.

Step 7: In the No Match Message field, you can create the message to be displayed if there are no records matching the search condition. You can insert fields from the form that the search is related to for configuring the message.

To save the defined search, click on Apply Changes. You can preview the result from the defined search to confirm the output of the search.

If the defined search query is inappropriate, no data will be displayed when the search is executed. A message indicating the defined search criterion is incorrect will be displayed.

You will have to configure a correct query for the defined search to work.

Note: To configure a defined search, you must have some understanding of how the logical operators in an SQL Query works and you must have some knowledge of database names.

If more than one form is related to the defined search, when you select 'Field Data to Use' action to configure Search Conditions or No Match Message, only field common to ALL related forms will be displayed.

Field Data to Use feature will not display any field if the defined search is related to Home form.

Frequently Asked Questions

This section lists questions you may encounter when configuring and managing Defined Searches. Click on a question to view its response.

Can the same defined search be used for more than one form?

Yes, a Defined Search can be related to multiple forms. The Related to form Lookup allows you to choose more than one form to which the defined search can be related.

Which are the fields to be displayed in the Field Data to Use Lookup window?

The fields on the form(s) that the defined search is related to get displayed in the Field Data to use lookup. This includes standard fields as well as Custom fields on the form.

Where a Defined Search is related to more than one form, the Field Data to Use lookup will display only those fields that are commonly available on all related forms.

Will I get an error message if a given search query is illogical or incorrectly framed?

No, you do not get any error message if you configure an incorrect or illogical search query. However, when you attempt to preview the data, you will get a message that the Defined Search Criteria is incorrect.

What happens when I change the query on an existing defined search? Are there any back impacts or other areas where the search is being used?

When you change the query on an existing defined search, the data output will be based on the newly defined query the next time the search is executed. If the defined search is used on a Chart, the output in the chart will change to match the new data from the new query.

There are no back impacts of modifying the Search Query if the search is correctly configured.

What happens when I delete a defined search that is already used and available to Agents?

Deleting a defined search that is already being used by Service Desk Agents will mean that the defined search will not be available to them thereafter.

The defined search will be taken off the list(s) where the search gets listed when active and available.

Chapter 32 – Manage Charts

Overview

Charts are a visual representation of information of at least two variables (say on the X and Y axis) to highlight their dynamic relationships. It is usually easier to process the visually depicted data than to read up the raw data that the chart is produced out of.

Users of Nimsoft Service Desk can access charts in the Home Page and in Dashboards configured to depict specific type of information. They can also drill down to view the record depicted in a portion of the chart.

For instance, if a user access a chart depicting Ticket Aging and the data depicts 4 tickets as being more than 7 days old, the user can click on that section of the chart to view the 4 tickets and can further drill down into each ticket to view further details.

Self-Service Users have access to a chart that depicts data on the Status of their tickets on the Home Page. Service Desk Agents can view three charts based on the Ticket List in the Home Page and in the List Tickets page in each ticket module. If permission is enabled, Service Desk Agents or Support Technicians can also view different charts in their dashboards.

As Application Administrator, you can view existing charts, configure new charts, and manage permissions for users, groups, and roles to access the charts.

Manage Charts

You can configure Charts from the Manage Charts link under Application Setup in the Navigation Menu. Clicking on this link displays the Manage Charts form and the Chart List tab. All Active Charts are listed in the tab.

You can search for a specific Chart by entering Chart name or create a new Chart. When you click on an existing chart in the list, the details get displayed in the Chart Details tab. You can also create a new chart in this tab.

The main fields in the Manage Chart form are listed below.

Field Name	Detailed Description
Chart Name	This is a required field, where you can specify a name for the Chart.
Description	This field allows you to provide a description that explains the data represented in the chart.
Auto-Refresh Interval	You can specify the interval at which the chart will be refreshed and rendered again.
Category	You can configure a category for the chart if you wish to categorize it in any way. You can create new categories, or use a category created earlier.
Chart Information	This section allows you to configure the various parameters of the chart.
Defined Search Name	This field allows you to choose the defined search that will be used to draw out data for the chart. Output of the defined search will be displayed in the chart.
Related To Form	This field gets auto-populated when you choose a defined search. It displays the form the defined search is related to.
Preview	You can use this action button to preview data represented in the chart.
Chart Type	You can select the chart type from the available options such as Line Chart, Bar Chart, Pie Chart, Area Chart, etc. The Show Legend and 3D check boxes allow you to further define how the data is represented.
Category (X-Axis)	You can use this field to define the information to be displayed in the X-Axis of the chart. You can choose a label for this field using the Category Label field.
Value (Y-Axis)	You can use this field define the information to be displayed in the Y-Axis of the chart. You can choose a label for this field using the Category Label field.
Time Period	This field allows you to specify a time period over which data is to be displayed. You can choose an appropriate value if required in context of the chart.
Aggregation	You can define the aggregation method for the chart by choosing an option from the Dropdown List. If an irrelevant option is selected, data will not be displayed.
Orientation	You can choose either vertical or horizontal orientation for the chart.

Permission	This tab allows you to manage Permissions for access to the chart for users, support groups, and Roles.

A chart renders data collected via a defined search. Based on the auto-refresh interval set, the defined search is executed again to collect fresh data; and the chart is rendered with the fresh data. If there is no record matching the defined search, the chart will be blank.

However, if any field value chosen is incorrect for an inappropriate category, value, or Aggregation option is chosen, a message indicating that that chart could not be rendered will be displayed.

The charts thus created become available for use in various dashboards that can be configured and made available for different users, support group, and roles. Some standard pre-configured charts are available as System-Defined charts. You cannot modify these charts.

You can, however, make a system defined chart as Inactive. As Application Administrator, you can manage access to a chart (both system-defined and non system-defined charts) for users, Support Groups, and roles. You can also manage the Status of a chart as active or Inactive. Only Active charts will be available for being used on a Dashboard.

Manage Charts Checkpoints

Some points to check when configuring charts are:

- A chart draws data from a defined search. Hence, a corresponding defined search is a pre-requisite for configuring a chart.
- If the defined search is incorrectly configured, the chart will fail to render relevant data.
- If a user does not have access to a defined search, the chart will not be rendered for that user.
- If inappropriate values are chosen for fields like category, value etc; the chart will not be rendered.

How Do I

Below are some actions you can take related to Custom charts.

Create new charts to be used on custom dashboards.

You can create new Charts and modify existing Charts from the Manage Charts link under Application Setup.

To Configure a new Chart:

Step 1: Click on the Manage Charts link under Application Setup. The Chart List will display a list of all active charts.

Step 2: Click on the Create New action button. A blank Manage Charts form will be displayed in the Chart Details tab.

Step 3: Enter a Name for the Chart in the Name field, which is a required field. You can add a description about the chart if you wish; and also choose a Category for the Chart. You can either choose a category from the existing list in the lookup or create a new category. However, these are not required fields and can be left blank. The Auto-Refresh interval is automatically set at default 3 minutes. You can modify this if required.

Step 4: Choose a Defined Search which will be used to draw out the data for the chart. You can preview the data to check if the defined search is configured correctly and displays appropriate data.

Step 5: Choose a Chart Type as appropriate for data to be displayed, from the dropdown list.

Step 6: Select the Category which will be displayed in the X-Axis and the Value to be displayed in the Y-Axis. This will control how the data is presented in the Chart. You can also choose Labels for the data in the X-Axis and Y-Axis if required. You can also choose to leave it blank.

Step 7: The next required field is Aggregation. You can choose how data is to be aggregated. The default is Count. You can choose alternatives like Average, Minimum, Maximum or Sum.

To save the Chart, click on Apply Changes. Further Chart details like Status, Created on, Created by, etc. get automatically updated.

The Chart will get displayed in the display section. You can modify the chart to change chart type, data type, aggregation etc. The chart will be refreshed based on the auto-refresh interval set.

Note:

A Defined Search is a pre-requisite to configuring a Chart. Hence you must check if the required data is available in an existing defined search or not. You can configure a new defined search for the chart if needed.

If an inappropriate combination is selected; like inappropriate value in the X-Axis and/or Y-Axis; inappropriate Aggregation etc, the Chart will not be rendered.

If there is no relevant data in the Defined Search, no chart will be rendered.

If a user does not have access to a Defined Search, the chart will not be rendered for the user.

Frequently Asked Questions

This section lists questions you may encounter when configuring or managing charts. Click on a question to view its response.

How many charts can I create?

There is no limit on the number of charts that you can create. You can create as many charts as you wish to display as dashboards.

Where can users see the charts that I create?

Users can see the charts you create in a dashboard on which the chart is used. All charts are available for the dashboards related to the same form. You can layout related charts in the dashboard to view real-time data.

When you configure the chart, the chart will get displayed in the Chart section of the form.

Can I create charts to be available to self-service users in the home section?

No, Charts cannot be configured to be viewed in the Self-Service User interface. They are accessible only from the My Dashboard link in the Agent/Administrator interface of the application.

Can I create a custom chart to be used in the Ticket Home pages by Agents?

No, the charts you see in the Home Page and List Tickets page of the ticket modules are system defined. A logged in user can only choose from the available charts to be displayed in the Home Page.

Can I use new/custom defined search for a Chart or am I limited to using only the out of box defined searches for a chart?

A pre-requisite for configuring a Chart is a Defined Search. The data that is displayed in the chart is a visual representation of the data drawn by SQL query in the Defined Search.

You can use either one of the available pre-configured defined searches, or use a defined search configured by you as the data source for the chart.

You can specify a refresh interval for the chart. Based on the refresh interval, the SQL is executed again, and fresh data is displayed.

A chart will fail to get rendered if the SQL query is incorrect or if the chart type or data fields are incorrectly selected.

Chapter 33- Manage Dashboards

Overview

Dashboards enable users to access real-time information on performance against established Key Performance Indicators. These key indicators ensure accountability and efficient functioning. Dashboards provide the business perspective in a very clear fashion and help to align us with strategic goals.

Nimsoft Service Desk provides a collection of individually tailored Key Performance Indicators such as Ticket Aging, performance related to SLA Compliance, etc. to create dashboards for different user Roles.

As Application Administrator you can define Key Performance Indicators and group them together to create various types of dashboards. Providing dashboard access to Service Desk Agents allows them to see their own tickets as well as group tickets while keeping a close eye on Resolution rate and SLAs. Service Desk Agents get an eagle's view into the overall health of the Service Desk.

Manage Dashboards

You can configure Dashboards from the Manage Dashboard link under Application Setup in the Navigation Menu. Clicking on this link displays the Manage Dashboard form and the Dashboard List tab.

All Active Dashboards are listed in this form. You can filter the list using the available filter options or search for a specific Dashboard by entering relevant information in the search window. When you click on an existing Dashboard in the list, the details get displayed in the Dashboard Details tab. You can also create a new Dashboard in this tab.

Application Setup (Manage Dashboards)
Manage Dashboard

Dashboard List | Dashboard Details

Dashboard #8: Task Dashboard

Copy To New | Apply Changes | Create New | Delete

Dashboard Name: Task Dashboard | Related To Form: Task Ticket | Status: Active

Description: My Dashboard | Created On: 7/7/2009 01:35:19 PM | Created By: Admin, IntaQ

Modified On: 7/7/2009 01:35:50 PM | Modified By: Admin, IntaQ

Context: ☒ Default ☐ Group ☐ User | Group / User: | Size (pixels): 250px x 200px

Grid Layout: 1 rows X 2 columns

Organize Dashboard Charts

1. My Tickets

2. Aging of Tickets

The main fields in the Manage Dashboard form are listed below.

Field Name	Detailed Description
Dashboard Name	You can specify a name as an identifier for the dashboard in this field.
Description	You can provide information that briefly describes the dashboard for the users.
Related To Form	You can specify the form that the dashboard is related to by choosing the form options in the look up associated with this field.
Context	This field is used to manage access to the dashboard for groups or users. System defined dashboards are available to all agents and administrators on their user Interface. For non-system defined dashboards access can be enabled for groups or users.
Grid Layout	You can manage the dashboard display by specifying number of charts to be displayed and the image size.
Organize Dashboard Charts	You can choose the charts that will be part of a dashboard; and the order in which the charts will be displayed from the Organize Dashboard pop-up.

Dashboards can be accessed from the My Dashboard link under Home in the Navigation Menu. You can enable or disable access to this link and thereby access to Dashboards for users, support groups, and Roles.

You can configure a Dashboard to display up to a maximum of 6 charts in a 2 X 3 grid. For a chart to be available as part of a dashboard, the chart related to the specific form has to be configured from the Manage Charts link. Only those charts that are related to the same form type as the dashboard will be available in the Organize Dashboard lookup.

For charts to be rendered on the dashboard, the defined search has to be configured and made available for the user. Similarly, access to the chart has to be enabled for the user. If access to either defined search or chart is not enabled for the user, the chart will not be rendered on the dashboard. A message indicating that the chart cannot be rendered will be displayed.

Manage Dashboards Check Points

Some points to check back on when managing dashboards are:

- A dashboard can be configured for any one Ticket type of related to Configuration Items.
- A dashboard is related to only one form type.
- Only those charts which are related to the same form as the dashboard are available for use on a dashboard
- The charts on the dashboard are auto-refreshed as per the interval set when configuring the Chart.
- For a dashboard chart to be available to a user or group, the associated defined search and chart have to be available as well.

How Do I

Below are some actions you can take related to custom Dashboards.

Configure a custom Dashboard

You can configure Dashboards to display performance against Key Performance Indicators for Ticket and Configuration Items. Dashboards can be configured using charts that display data based on defined searches.

You can configure Dashboards from the Manage Dashboards link under Application Setup. To Configure a Dashboard:

Step 1: Click on the Manage Dashboard link under Application Setup. A list of Active Dashboards will be listed in the Dashboard List tab.

You can click on an existing Dashboard to view details of the Dashboard. The Dashboard will be displayed in the Dashboard Details tab.

Step 2: Click on Create New to create a new Dashboard. You can also choose to Copy an existing Dashboard and modify it to create a new Dashboard.

Step 3: Enter a Name for the Dashboard in the Name field, which is a required field.

You can add a description about the chart if you wish. However, this is not a required field and can be left blank.

Step 4: Choose which form a Dashboard will be related to. You can choose only one from the dropdown list.

Step 5: In the Context field; choose whether the access to the Dashboard is to be assigned to Group or Users. Depending on the context selected, the List of Groups or List of Users will be displayed in the Groups/Users field. Select the Users or Groups to whom the Dashboard will be available.

Default Context is disabled for dashboards configured by the administrator. Default context applies only to System-defined dashboards.

Step 6: Select the Grid Layout for the Dashboard. You can display a maximum of 6 charts in a 2X3 grid; and a minimum 1 chart in a 1x1 grid.

You can also modify the chart size by managing the image pixels.

Step 7: Click on the Organize Dashboards action button. A list of available Dashboard Charts will be displayed. From this list, select charts to be displayed in the Dashboard.

You can manage the layout of the charts, the order in which they appear etc. from the Organize Dashboard lookup by moving the charts up or down the list.

Step 8: To save the Dashboard, click on Apply Changes. Dashboard details like Status, Created on, Created by, etc. get automatically updated.

The Charts that are part of the Dashboard will get displayed in the display section.

Users can manage their own dashboard by modifying grid layout and selecting for available charts.

Note:

To configure a Dashboard, relevant charts have to be configured from the Manage Dashboard Section. Hence configuring Charts is a pre-requisite to configuring a Dashboard.

Users can access the Dashboard from the My Dashboard link under Home. If permission to the My Dashboard link is not enabled, users will not be able to view a dashboard even if the user/group is selected in the Dashboard Context.

If a user does not have access to a defined search used to render a chart, the chart will not be displayed in the dashboard. A message will be displayed in place of the chart.

Frequently Asked Questions

This section lists questions that you may encounter when managing Dashboards. Click on a question to view its response.

Can Agents create new dashboards for themselves?

Agents can access dashboards only if permission to My Dashboards link is enabled for them.

If access to this link is permitted, Agents can manage their own Dashboard views by laying out available charts in the dashboard, selecting from among available charts, etc.

They cannot create new charts to be used in the dashboard. They can only choose from available charts for which permission has been enabled by the application administrator.

Can I create a dashboard with a combination of custom defined and system defined charts?

Yes, you can configure a chart using a combination of system defined and non-system defined charts.

Agents can also use both system defined and non-system defined charts in their dashboard so long as permissions to access the charts has been enabled.

Can an agent view all dashboards that I create?

When configuring dashboard, there is an option of Context, which allows you to select Group or User. The dashboard will be available to the Group or Users identified in this field.

Therefore, a Dashboard is not visible by default to all users.

Can I change the number of charts in a dashboard?

You can choose a maximum of up to 6 charts in a dashboard for a grid layout of 2X3. You can choose less than this (2X2 or 1X2), as required.

Thus you can choose from between 1-6 charts for a Dashboard.

Can I set the same Dashboard for more than one form?

No, a dashboard can be related to only one form. The Related to Form dropdown will not allow you to relate a dashboard to more than one form.

Chapter 34 – Trends and Metrics

Overview

Organizations use reports to manage service delivery and operational effectively. Reports are an effective way to measure performance and track and identify the obstructions that are affecting performance. They enable you to work efficiently and improve end-user satisfaction by keeping track of trends and measuring performance.

Nimsoft Service Desk provides you access to a range of reports related to Ticket, Configuration Items and Service Level Management. These reports can be accessed in the Trends and Metrics section in the Navigation Menu.

The primary focus of the reports is to provide useful and ready-to-use reports. These reports are designed to:

- Present to you information of interest
- Group and categorize information for instant analysis
- Specify the report to be visible for a time period of choice
- Present a measured snapshot of the organizational performance

Features of Reports

The following reports represent different kinds of data or same data in different formats:

- You can view data on various aspects of a ticket like aging analysis, Ticket by Status, ticket volume and backlog, etc.
- You can extract reports for individual aspects of a ticket, like work efforts over a chosen period, volume against work efforts, etc.
- Reports are grouped and categorized for more effective presentation of information and enhanced usability.
- Reports can be grouped by Organization, Assigned to Support Group, Assigned to Individual, etc.
- You have the option to change the Report Date as well as the Start and End Date for a Period report and execute the report again.

- You have the option to view the Report on Screen or Export it in PDF or CSV format.
- You can view Bar Charts and Pie Charts associated with each report that are displayed along with corresponding data in Tabular format.

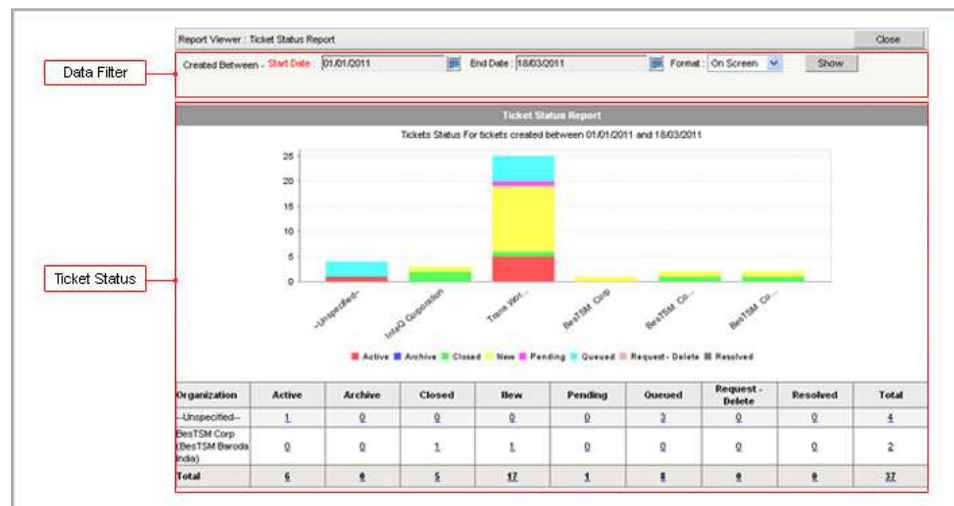
Types of Reports

Reports are grouped under different heads in the Trends and Metrics section. You can change this grouping from the Manage Report Configuration link under Administration Utilities in the Navigation Menu. The available grouping and reports grouped by default are:

Executive Summary

Executive Summary Reports display data on various aspects of a ticket. Such reports provide basically operational information related to a time instant (Snapshot Report) or covers specific time duration (Period report).

By default, a Snapshot report is based on the current date. A Period report covers last week (Current Date -7 days to current date). It will show both the Created Between Start Date and the End Date. For example, a report for November 22, 2008, will be Created Between Start Date November 16 and End Date November 22.



You can access a variety of Executive Summary reports from the link under Trends and Metrics.

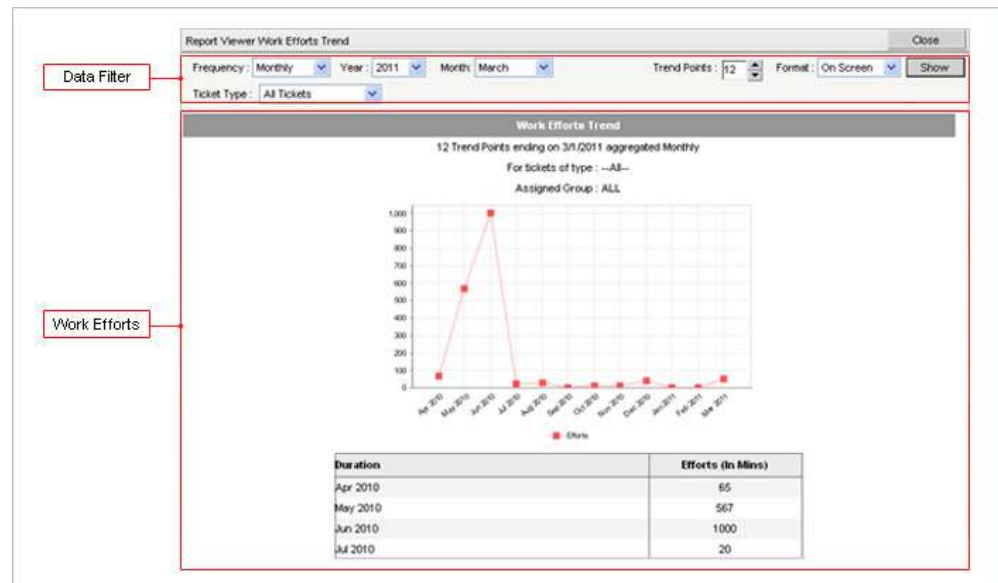
For example, you can view and generate Tickets with Open Tasks Report to see all changes that have open tasks during the selected reporting period.

While generating this report you can choose Task Ticket planned start and end date range, Task Ticket template and Change Type in Change Requests. Similarly, you can generate the All Open And Closed Tickets report to report the time logged by Analysts/Agents for a specific Organization or Site during the selected reporting period. These reports are also available for each ticket module.

Delivery Trends

These reports provide information related to Volumes, Back logs, and Effort over a period of time. Trend reports are conceived in terms of covering several periods in past for example, last X days, last X weeks or last X months.

You can plot a trend for the past 1 to 12 days, weeks or months. Delivery Trend reports present data based on the trend analysis on the work delivered by a specific group. The report can be displayed for any or all Ticket types, for a specific group, and specified trend points.



Reports related to Delivery Trends are grouped together under Delivery Trends Reports under Trends and Metrics section in the Navigation Menu.

Top 5

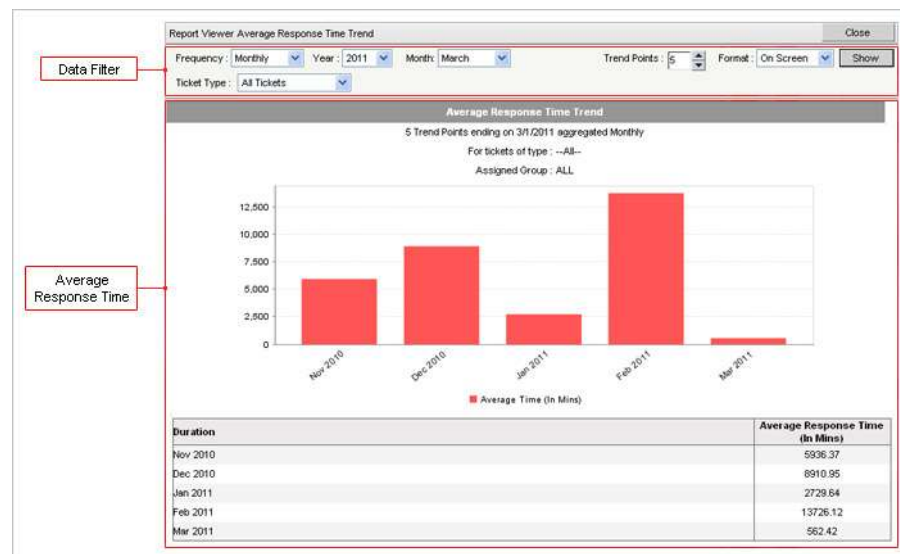
These are Pareto Reports based on Top 5 sources of number of tickets. They display information based on Organization, Requester, Categorization (CCTI), and Services. The displayed data in the reports can be changed according to a specified Start and End Date.



The Top 5 Reports provide data that can be used to identify top Ticket requester, support, requesting organizations, etc. These reports are grouped together in a section called Top 5 Reports in the Trends and Metrics section in the Navigation Menu.

Service Level Trends

These reports display the average data such as Average Response Time, Average Resolution Time, and Average Time to Close a Ticket, etc. As in deliver Trend reports, these reports too can be displayed for any or all Ticket types, for a specific group, and specified trend points.



These reports related to performance of the Service Desk against established Service Level Agreements can be accessed from the Service Level Trends group under Trends and Metrics in the Navigation Menu.

Available Reports

The table below provides details of all reports that are available out-of-the box. The list indicates the default grouping assigned to the reports.

Report Name	Related to Form(s)	Description	Category	Key Variables
Ticket Volume and Background Trends	Home	Displays a trend analysis showing the volume of incoming tickets against number of tickets resolved and tickets pending resolution (backlog) during the specified reporting period.	Delivery Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points, Ticket Type
Ticket Volume and Background Trends by Group	Home	Displays trend analysis per Support Group, showing the volume	Delivery Trends	Frequency (including relevant parameters for Daily, Weekly,

		of incoming tickets against the number of tickets resolved and tickets pending resolution (backlog) during the specified reporting period		Monthly), Trend Points, Ticket Type, Assigned to Group
Ticket Volume and Background Trends by Individual	Home	Displays trend analysis per Support Technician (Agent), showing the volume of incoming tickets against the number of tickets resolved and tickets pending resolution (backlog) during the specified reporting period	Delivery Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points, Ticket Type, Assigned to Individual
Work Effort Trends	Home	Displays a trend analysis showing the total time spent (in mins) on tickets during the specified reporting period	Delivery Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points, Ticket Type
Work Effort Trends by Group	Home	Displays a trend analysis per Support Group, showing the total time spent (in mins) on tickets during the specified reporting period	Delivery Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points, Ticket Type, Assigned to Group
Work Effort Trends by Individual	Home	Displays a trend analysis per Support Technician (Agent) showing the total time spent (in mins) on tickets during the specified reporting period	Delivery Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points, Ticket Type, Assigned to Individual
Open Tickets Aging Report	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays details of open tickets for all Organizations in different aging periods during the	Executive Summary	Start Date, End Date

		selected reporting period. The details are grouped by Organization		
Open Tickets Aging by Group	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays details of all open tickets assigned to different Support Groups, in different aging periods during the selected reporting period.	Executive Summary	Start Date, End Date, Reporting Date
Open Tickets Aging by Individual	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays details of all open tickets assigned to different Support Technicians (Agents), in different aging periods during the selected reporting period.	Executive Summary	Start Date, End Date, Reporting Date
Ticket Status Report	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays the total number of tickets, grouped by Organization, in different statuses	Executive Summary	Start Date, End Date
Ticket Status Report by Group	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays the total number of tickets, assigned to different Support Group, in different statuses	Executive Summary	Start Date, End Date
Ticket Status Report by Individual	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays the total number of tickets, assigned to different Support Technicians (Agent), in different statuses	Executive Summary	Start Date, End Date, Individual Name
Ticket Volume and Backlog Report	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays a organization-wise comparison of the number of incoming tickets versus the	Executive Summary	Start Date, End Date

		total tickets resolved and tickets pending resolution (backlog) during the specified reporting period		
Ticket Volume and Backlog Report by Group	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays a Support Group-wise comparison of the number of incoming tickets versus the total tickets resolved and tickets pending resolution (backlog) during the specified reporting period	Executive Summary	Start Date, End Date
Ticket Volume and Backlog Report by Individual	Home, Change, Incident, Problem, Service Request, Task Ticket	Displays a Support Technician-wise (per Agent) comparison of the number of incoming tickets versus the total tickets resolved and tickets pending resolution (backlog) during the specified reporting period	Executive Summary	Start Date, End Date
Work Efforts Report	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the total time spent (in mins) on tickets for different Organizations in the specified reporting period.	Executive Summary	Start Date, End Date
Work Efforts Report by Group	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the total time spent (in mins) on tickets by different Support Technicians in the specified reporting period.	Executive Summary	Start Date, End Date
Work Efforts Report by Individual	Change Request, Home, Incident, Problem, Service	Displays the total time spent (in mins) on tickets by	Executive Summary	Start Date, End Date

	Request, Task Ticket	different Support Technicians (Agents) in the specified reporting period.		
Average Response Time	Change Request, Home, Incident, Service Request	Displays the average time taken to send an acknowledgement back for tickets logged by Requester Organization and Sites.	Executive Summary	Start Date, End Date
Average Response Time by Group	Change Request, Home, Incident, Service Request	Displays the average time taken by different Support Groups to send an acknowledgement back for tickets logged.	Executive Summary	Start Date, End Date
Average Response Time by Individual	Change Request, Home, Incident, Service Request	Displays the average time taken by different Support Technicians (Agents) to send an acknowledgement back for tickets logged.	Executive Summary	Start Date, End Date
Average Response Time by Configuration Items	Change Request, Home, Incident, Service Request	Displays the average time taken to send an acknowledgement back for tickets based on Configuration Items related to the ticket.	Executive Summary	Start Date, End Date
Average Resolution Time	Change Request, Home, Incident, Service Request	Displays the average time taken to provide a resolution for tickets logged, grouped by	Executive Summary	Start Date, End Date

		Requester Organization and Sites		
Average Resolution Time by Group	Change Request, Home, Incident, Service Request	Displays the average time taken by different Support Groups to provide a resolution for tickets assigned to the Support Group.	Executive Summary	Start Date, End Date
Average Resolution Time by Individual	Change Request, Home, Incident, Service Request	Displays the average time taken by different Support Technicians (Agents) to provide a resolution for tickets assigned to the technician.	Executive Summary	Start Date, End Date
Average Resolution Time by Configuration Items	Change Request, Home, Incident, Service Request	Displays the average time taken to provide a resolution for tickets based on Configuration Items related to the ticket.	Executive Summary	Start Date, End Date
Average Time to Close Tickets	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays average time taken to close tickets grouped by Requester Organization and Site.	Executive Summary	Start Date, End Date
Average Time to Close Tickets by Groups	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the average time taken by different Support Groups to close tickets assigned to the group.	Executive Summary	Start Date, End Date
Average Time to Close Tickets by Individual	Change Request, Home, Incident, Problem, Service Request, Task	Displays the average time taken by different Support	Executive Summary	Start Date, End Date

	Ticket	Technicians (Agents) to close tickets assigned.		
Average Time to Close Tickets by Configuration Items	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the average time taken to close tickets grouped by the Configuration Item related to the ticket.	Executive Summary	Start Date, End Date
Service Level Breach History Report	Home	Displays historical data of tickets logged against tickets that have breached SLA Targets for selected Service Metrics during the selected reporting period.	Executive Summary	Start Date, End Date, Assigned to Group, SLA Metric
Service Level Breach History Report by Target	Home	Displays historical data of tickets logged against tickets that have breached SLA Targets for selected Service Targets during the selected reporting period	Executive Summary	Start Date, End Date, Assigned to Group, SLA Target
Service Level Compliance History Report	Home	Displays historical data of tickets logged against tickets that have met (Complied with) SLA Targets for selected Service Metrics during the selected reporting period	Executive Summary	Start Date, End Date, Assigned to Group, SLA Metric
Service Level Compliance History Report by Target	Home	Displays historical data of tickets logged against tickets that have met (complied with) SLA Targets for selected Service Targets during the	Executive Summary	Start Date, End Date, Assigned to Group, SLA Target

		selected reporting period		
Average Service Delivery Performance	Home	Displays the average service delivery performance conveying the SLA compliance levels for different ticket types against pre-defined Service Targets.	Executive Summary	Start Date, End Date, Requester's Organization, SLA Target, Affected Service, Exclude Tickets with In Progress Target, Include tickets created or closed during the report period.
Average Service Delivery Performance by Organization	Home	Displays the average service delivery performance conveying the SLA compliance levels for different ticket types against pre-defined Service Targets, classified by organization site.	Executive Summary	Start Date, End Date, Requester's Organization, SLA Target, Affected Service, Exclude Tickets with In Progress Target, Include tickets created or closed during the report period.
Average Service Delivery Performance by Service	Home	Displays the average service delivery performance conveying the SLA compliance levels for different ticket types based on Affected Services.	Executive Summary	Start Date, End Date, Requester's Organization, SLA Target, Affected Service, Exclude Tickets with In Progress Target, Include tickets created or closed during the report period.
Average Service Delivery Performance for Support Group	Home	Displays the average service delivery performance conveying the SLA compliance levels for each support group against the support group's service performance	Executive Summary	Start Date, End Date, Requester's Organization, SLA Target, Affected Service, Exclude Tickets with In Progress Target, Include tickets created or closed during the report period.

		targets for each ticket type		
Average Service Delivery Performance for Support Group by Organization	Home	Displays the average service delivery performance for different Organizations, conveying the SLA compliance levels for each support group against the support group's service performance targets for each ticket type.	Executive Summary	Start Date, End Date, Requester's Organization, SLA Target, Affected Service, Exclude Tickets with In Progress Target, Include tickets created or closed during the report period.
Average Service Delivery Performance for Support Group by Service	Home	Displays the average service delivery performance against selected Services, conveying the SLA compliance levels for each support group against the support group's service performance targets for each ticket type	Executive Summary	Start Date, End Date, Requester's Organization, SLA Target, Affected Service, Exclude Tickets with In Progress Target, Include tickets created or closed during the report period.
Ticket Status Report by Configuration Item	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the total number of tickets in different statuses, classified by Configuration Items related to tickets.	Executive Summary	Start Date, End Date, CCTI Class, Configuration Item
Ticket Status Report by Affected Services	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the total number of tickets in different statuses classified by Affected Services related to tickets.	Executive Summary	Start Date, End Date, CCTI Class, Affected Service
Tickets Details Report	Change Request, Home, Incident, Problem, Service	Displays ticket details like ticket general	Executive Summary	Created Between, Organization, Submitted by,

	Request, Task Ticket	information, additional information, worklog related to the support request.		Assigned Individual, Ticket Type, Class, Status
Ticket Activity by Individual	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the total number of tickets on which some activity was performed by individual Support Technician during the reporting period	Executive Summary	Individual Name, Start Date and End Date
Tickets with Open Tasks	Change, Home, Incident, Problem, Service	Displays support tickets with Open Child Task tickets during the selected reporting period.	Executive Summary	Planned Start Date, Planned End Date, Task Name (Task Group, Task Flow)
All Open and Closed Tickets	Change, Home, Incident, Problem, Service	Displays data for tickets created and closed, grouped by Requester Organization and Site, during specified reporting period.	Executive Summary	Created Between, Closed Between, Reporting Period Start Time, Ticket Organization, Ticket Site
Ticket Volume by CCTI	Change, Home, Incident, Problem, Service, Task	Displays volume of incoming tickets classified by Class, Category, Type and Item, logged during a specified reporting period.	Executive Summary	Start Date, End Date, CCTI Class
Configuration Items Details Report	Configuration Items	Displays a list of all Configuration Items along with associated custom CI attributes	Executive Summary	Start Date, End Date, CCTI Class, Attribute Name
CI Status Report	Configuration Items	Displays information on Configuration Items in different statuses, classified by organization and	Executive Summary	Report as on Date

		site.		
CI Status Report by Class	Configuration Items	Displays information on Configuration Items in different statuses, classified by Class and Category	Executive Summary	Report as on Date
CI Warranty Expiry Report	Configuration Items	Displays a list of Configuration Items where the Warranty is due to expire during the specified month, or two subsequent months from the month specified	Configuration Item Reports	Year, Month
CI Related Open Tickets Report	Configuration Items	Displays the total number of open tickets related to Configuration Items, grouped by the CI classification (class-category).	Configuration Item Reports	Report Date
Top 5 CCTI Report	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays top 5 classification (CCTI) associated with tickets logged during the selected reporting period.	Top 5	Start Date, End Date
Top 5 Requesters Report	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays the top 5 requesters, submitting the maximum number of tickets during the selected reporting period.	Top 5	Start Date, End Date
Top 5 Organizations Report	Change Request, Home, Incident, Problem, Service Request, Task Ticket	Displays top 5 organizations with maximum number of tickets submitted during the reporting period.	Top 5	Start Date, End Date
Top 5 Services Report	Change Request, Home, Incident,	Displays top 5 services that were	Top 5	Start Date, End Date

	Problem, Service Request, Task Ticket	associated as Affected Services with maximum number of tickets logged during the reporting period.		
Average Response Time trends for Self-Service Users	Service Request	Displays a trend analysis showing the time taken to send an acknowledgement back for tickets requested by or requested for a specified self-service user during the selected reporting period.	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly Monthly), Trend Points
Average Resolution Time trends for Self-Service Users	Service Request	Displays a trend analysis showing the average time taken to provide a resolution for tickets requested by or requested for a specified self-service user during selected reporting period	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly Monthly), Trend Points
Average Response Time Trend	Home	Displays a trend analysis showing the time taken to send an acknowledgement back for tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type
Average Response Time Trends by Individual	Home	Displays a trend analysis showing the time taken by Support Technicians (Agents) to send an acknowledgement back for tickets during the past X	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Assigned to Individual.

		days, weeks, or months.		
Average Response Time Trends by Group	Home	Displays a trend analysis showing the time taken by Support Groups to send an acknowledgement back for tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Assigned to Group
Average Response Time Trends by Configuration Item	Home	Displays a trend analysis showing the time taken to send an acknowledgement back for tickets during the past X days, weeks, or months classified by the Configuration Item related to the ticket	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Configuration Item
Average Resolution Time Trend	Home	Displays a trend analysis showing the average time taken to provide a resolution for tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type
Average Resolution Time Trend by Individual	Home	Displays a trend analysis showing the average time taken by Support Technicians (Agents) to provide a resolution for tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Assigned to Individual
Average Resolution Time Trend by Group	Home	Displays a trend analysis showing the average time	Service Level Trends	Frequency (including relevant parameters for

		taken by Support Groups to provide a resolution for tickets during the past X days, weeks, or months		Daily, Weekly, Monthly), Trend Points. Ticket Type, Assigned to Group
Average Resolution Time Trend by Configuration Items	Home	Displays a trend analysis showing the average time taken to provide a resolution for tickets during the past X days, weeks, or months classified by the Configuration Item related to the ticket	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Configuration Item
Average time to close tickets trend	Home	Displays a trend analysis showing the time taken to close tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type
Average time to close tickets trends by Individual	Home	Displays a trend analysis showing the time taken by Assigned to Support Technician (Agent) to close tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Assigned to Individual
Average time to close tickets trends by Group	Home	Displays a trend analysis showing the time taken by assigned to Support Group to close tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type, Assigned to Group
Average time to close tickets trends by Configuration Items	Home	Displays a trend analysis showing the time taken to close tickets during the past X days, weeks, or months	Service Level Trends	Frequency (including relevant parameters for Daily, Weekly, Monthly), Trend Points. Ticket Type,

		classified by Configuration Items related to the ticket		Configuration Item
Knowledge Article by Category	Home	Displays various usage metrics for Knowledge Articles, classified by category, that help you monitor your knowledge base activity for identifying Knowledge Articles created, published and updated and popularity of articles based on views, ratings and usefulness in solving most reported cases.	Knowledge Management Reports	Modified Between, KB Article Category
Service Feedback Analysis	Home	Displays an interpretation and analysis of the quantitative customer service satisfaction survey data to enable measurement and necessary service improvements based on the feedback received.	Survey Reports	Schedule Name, Include Response details, Include Charts
Scheduled Changes	Change Request	Displays all planned changes scheduled for the selected reporting period	Change Management Reports	Start Date, End Date
Scheduled Changes by Individual	Change Request	Displays all planned changes assigned to a Support Technician (Agent) during the selected reporting period	Change Management Reports	Frequency (including relevant parameters for Daily, Weekly Monthly), Trend Points, Assigned To Individual
Scheduled Changes	Change Request	Displays all planned	Change	Frequency

by Group		changes assigned to a Support Group during the selected reporting period.	Management Report	(including relevant parameters for Daily, Weekly Monthly), Trend Points, Assigned To Group

Besides accessing the tickets from the Trends and Metrics module, they can also be accessed from the various Ticket Modules, Configuration Management Module, Knowledge Management Module and Service Feedback Module as relevant. Access to the reports can be managed by enabling or disabling permissions.

Manage Reports Permissions

Reports are more useful to roles that involve review and monitoring of performance and for ensuring service delivery standards. Access to the Trends and Metrics module is, therefore, most useful for a group or role designated for this purpose.

Based on the need for reports, access to the Trends and Metrics module (or relevant reports) can be provided to roles responsible for periodic extraction of reports or roles that use reports for planning and analysis.

The reports are grouped into the categories for ease of access and use. However, you can choose to regroup the reports in any other category from the Manage Report Configurations link under Administration Utilities. This link allows you to configure new reports; modify aspects of existing reports like Report Description, Related to form, and Report Category Name.

You can manage access to the Trends and Metrics section (and to all report groups under this section) by managing permission to the module and relevant Report sections in the Navigation Menu.

You will also need to enable access to individual reports to an individual, support group or role; as relevant.

How Do I

Below are some actions you can take related to reports.

Extract a Report from the list

Nimsoft Service Desk allows you to generate a range of reports related to Tickets, Configuration Items, Knowledge Articles and Service Feedback. You can view and extract reports related to a range of Service Desk Operations.

To extract a report

Step 1: Go to the Reports link under the appropriate application Module (like Request Management, Knowledge Management, Trends and Metrics etc.)

For example, if you want to extract a report related to Service Level Compliance for Tickets which is available under Executive Summary section under Trends and Metrics; click on Trends and Metrics to view the links in this module. Click on Executive Summary to view reports grouped into this category.

Step 2: From the list of available reports, select the report you would like to extract.

The report will open in a new window. The Key Variables for the report; or data elements that you can choose will be displayed as a lookup or dropdown fields.

Step 3: Choose the reporting period (date range) and other variables. Choose whether you want to view the report on screen or would like to extract it into a PDF or CSV File.

Step 4: Click on Show and the report will be generated in the format desired.

If you have chosen On Screen, the report will be displayed. If not, a dialogue box prompting you for the location where the PDF or CSV file is to be saved will be displayed.

Note:

Grouping of the reports can be changed from the Manage Report Configuration section. Access to the report is controlled from Manage Report Configuration and Manage Navigation Menu links.

Enable Access to a report or set of reports

Nimsoft Service Desk provides you access to a range of reports related to Tickets, Configuration Items, Knowledge Management and Service Feedback. You can allow access to these reports for Service Desk Agents, if required.

You can enable access to reports to a Contact, Support Group or Role. To enable access to a report:

Step 1: Click on the Manage Report Configurations link under Administration Utilities. A list of all available reports will be displayed.

Click on a report from the list. The details will get populated in the form below. You can manage access to the report from the Permissions Tab.

Step 2: Click on Permissions tab. A list of users, support groups and roles to whom permissions is enabled will be listed.

Step 3: Click on the Manage Permission action button to open the Permission Editor lookup.

Step 4: Choose names of contacts from the "Select the permissions to be granted" list and click Add. The chosen names get displayed in the list under "Current Permission".

You can also revoke permissions granted from this lookup.

Step 5: Click Close to close the Permission Editor.

A list of all users, support groups, and roles who can access the report will be displayed.

Service Desk Agents, who have permissions to the Reports link under the appropriate module and permissions to access the individual report, will be able to extract the report.

Note:

Service Desk Agents can view reports for that module from the Reports link under each related module. If access to the Report link for that particular module is not enabled, Service Desk Agents will not be able to access the report even if permission to the individual report is enabled.

You can also choose to grant permissions to the Trends and Metrics Module to contacts by enabling permission to the Module from the Manage Navigation Menu form.

Frequently Asked Questions

This section lists questions you may have regarding the Trends and Metrics module.

Can I change the reports grouping?

Yes, you can modify the grouping applied to a report by selecting the report you wish to modify from Manage Report Configuration link under Administration Utilities.

You can choose which group the report should appear under from the Category Name lookup and apply changes. The report will now become available in the newly set group.

Can I delete a report that is visible in any group?

Yes, you can delete a report that is visible in any group by selecting the report you wish to delete from the Manage Reports Configuration link under Administration Utilities.

Deleting a report will result in its being removed from all places where it is listed.

Can Agents access the reports visible in the Trends and Metrics Section?

Agents can access the Trends and Metrics Module and all reports listed in that section if permission to access the section and permission for the reports listed is enabled. You can enable access to this module from the Manage Navigation Menu link under Administration Utilities.

While access to the Trends and Metrics Module is not needed for all Agents, access to this Module is particularly useful for those contacts who are involved in managing or supervising IT Operations. You could therefore, configure a Support Group or Role for such contacts and assign permission for access to the Trends and Metrics Module for contacts who are members of this Support Group/Role.

In what formats can I generate a report?

The reports accessible from the Trends and Metrics Module and all other Modules across the application can be viewed On Screen. To extract the report, you can extract the report in PDF or CSV formats.

Can I add new reports to the various groups of reports under Trends and Metrics?

You can configure new reports using existing Report Key and select which group the report will appear in the Trends and Metrics section. However, please note that you cannot create a new Report Key as the data in the report could be a duplicate of another existing report.

Chapter 35 – Manage Config Parameter

Overview

Service Desk operations are managed differently in each Organization. While some customers would want certain features, other customers would not wish to enable a given feature, or would want to use it in a different way.

Nimsoft Service Desk allows individual customers to manage a wide range of functionality to suit their distinct need. To enable the application administrator to enable or disable a feature or functionality, or modify a functionality in some limited way, a range of functions that can be modified are made available under Manage Config Parameters in the Application Setup Section of the Administration User Interface.

You can view all Configurations Parameters under Application Setup section in the Navigation Menu. You can filter the list based on parameter category to view the parameter you would like to modify. The most commonly used variation or a parameter is available as default. You can customize a Slice by selecting an alternative variation to suit the needs of your organization.

Each Slice Configurations has a parameter with specified values to define its role and behavior. A parameter value can be in the form of a Boolean variable, a number, an URL, a list depending upon the kind of Role performed by the Parameter, etc.

This section lists all Configuration Parameters grouped together per parameter category. It also contains an explanation of what the parameter controls, which user(s) get affected by the parameter, the parameter default value, and alternate values possible.

Config Parameters

You can access the Configurations Parameters from the Manage Config Parameters link under Application Setup in the Navigation Menu. Clicking on this link displays the Manage Config Parameter form.

The list displays all Slice Parameters. Clicking on any parameter will populate the form below; and you can modify the parameter value as appropriate. You can also filter the list to view a listing per parameter category.

Form Name: % Application Setup (Manage Slice Configuration)

Parameter List:

ID	Parameter Category	Parameter Name	Parameter Value
525	Problem Management	PRB_ENABLE_CUSTOM_FIELDS	No
526	Tasks	TSK_ENABLE_CUSTOM_FIELDS	Yes
565	Incident Management	INC_DEFAULT_ASSIGNMENT_GROUP	45
580	Request Management	SRO_REQUESTER_REPLY_STATUS	
581	Change Management	CHO_REQUESTER_REPLY_STATUS	
582	Incident Management	INC_REQUESTER_REPLY_STATUS	
583	Problem Management	PRB_REQUESTER_REPLY_STATUS	

Record(s) 61 to 90 of 130

Parameter Details:

Parameter Category: Request Management

Parameter Name: SRO_REQUESTER_REPLY_STATUS

Parameter Description: Defines the status to be set on the service desk ticket when an email response is received from ticket's requester/requested-for contact or it is manually updated by a self-service user.

Parameter Value: Active

The Configuration Parameters are grouped under different Parameter Categories, based on the actions they control or the form they are applicable to. You can refer to the list below to view details of the available Configuration Parameters.

All Tickets (Service Desk)

The following Configuration Parameters are applicable to all tickets, and control how Service Desk works with tickets. These parameters are classified under Parameter Category "Service Desk" in the Manage ConfigU Parameters form.

MAX_ATTACHMENT_SIZE

This parameter controls the file size for attachments used across the Nimsoft Service Desk.

Title	Description
Parameter Name	MAX_ATTACHMENT_SIZE
Parameter Description	Sets the maximum file size (in MB) allowed for attachments, wherever the attachment functionality is available across the application
Default Value	3
Valid Value	Positive Integer
Impact Area	Under Attachment tab of various forms like Organization, tickets, Knowledge Article, CI etc.

Appears on Interface	All Users

REQUIRE_TIME_TRACKING_ON_ALL_TICKETS

This parameter manages Time Tracking functionality to enable time spent on individual worklog and collective time spent on a ticket.

Title	Description
Parameter Name	REQUIRE_TIME_TRACKING_ON_ALL_TICKETS
Parameter Description	If the parameter value is set to "Yes" the "Time Spent" & "Total Time Spent (HH:MM)" field will be displayed in the General Information Tab alongside Worklog related fields. Time tracking fields will also be shown when adding a worklog from the Activity Tab of a Ticket. Select "No" to hide the "Time Spent" & "Total Time Spent (HH:MM)" fields.
Default Value	Yes
Valid Value	Yes / No
Impact Area	All Tickets - Time Spent field associated with each Worklog entry
Appears on Interface	Agents

COMMUNICATION_TEMPLATES_OMITTED_DURING_EMAIL_DIVERSION

This parameter controls notifications diverted when a contact sets an 'Out of Office' flag, diverting notifications to a deputy.

Title	Description
Parameter Name	COMMUNICATION_TEMPLATE_OMITED_DURING_EMAIL_DIVERSION
Parameter Description	This parameter lists the ID numbers of Communication Templates. Notification Emails based on these Templates will not be redirected to the Deputy/ Alternate of a contact when the 'Out of Office' flag is set for the contact. The Notifications for these templates shall continue be delivered to contact going out of Office. The Contact can view the notifications in their Email.

Default Value	-1,-12,-17,-18, and -21
Valid Value	Communication Template ID
Impact Area	Email Notifications
Appears on Interface	Not Visible on GUI

REQUIRE_CASE_ID_GENERATION_FOR_ALL_TICKETS

This parameter controls Case ID generation for tickets. Depending on the parameter value, a unique Case ID will be generated for all tickets, and cases with a related Case ID can be tracked.

Title	Description
Parameter Name	REQUIRE_CASE_ID_GENERATION_FOR_ALL_TICKETS
Parameter Description	If the parameter value is set to "Yes", a unique Case ID is generated for all ticket types. This Case ID - Ticket ID combination becomes the unique identifier for a Ticket. The 'Move to Case' action for tickets enables associating a Ticket to a different Case ID. Set the parameter value to "No" to disable Case ID generation. In this case, unique Case ID will not be generated. A common series is used for each ticket type; for example, all Service Requests shall be 100-Ticket ID, all Incident Tickets shall be 200-Ticket ID, etc.
Default Value	Yes
Valid Value	Yes / No
Impact Area	Case ID number on all ticket types
Appears on Interface	All Users

APPLY_LIFECYCLE_PHASE_FOR_TICKETS

This parameter controls application of the concept of Ticket Phase.

Title	Description
Parameter Name	APPLY_LIFECYCLE_PHASE_FOR_ALL_TICKETS
Parameter Description	If the parameter value is set to "Yes", the Phase field is displayed on the ticket form for all ticket types. In addition to the basic fields of Ticket Status and Reason Code, 'Phases' for the life cycle of each ticket type can be defined and incorporated in configuration of Workflow Action Options and Auto Routes. Ticket Approval process, Ticket Advance Search, Predefined search, Reports, etc. can also incorporate the Phase field. If the value is set to "No" the Phase field is not displayed on tickets. However, Phase can still be used in configuring various functions such as Workflow action options and auto routes.
Default Value	Yes
Valid Value	Yes / No
Impact Area	All Tickets – Workflow configurations for Ticket Life cycle management
Appears on Interface	Agents

ENABLE_SLA_MONITORING_ON_TICKETS

This parameter manages SLA Monitoring on Tickets.

Title	Description
Parameter Name	ENABLE_SLA_MONITORING_ON_TICKETS
Parameter Description	If this parameter value is set to "Yes" to permit SLA Monitoring of tickets. When the value is set to Yes, the SLA Monitoring Tab is displayed on tickets. Information related to performance of the ticket against Service Targets defined, and notification, escalation and action on SLA Threshold Violation can be seen in this tab. Set the parameter value to "No" to disable SLA Monitoring. SLA Compliance will not be monitored and the SLA Compliance

	Tab on the tickets will not be displayed.
Default Value	Yes
Valid Value	Yes / No
Impact Area	All Tickets – SLA Information Tab
Appears on Interface	Agents

DEFAULT_REQUESTER_TO_LOGGED_IN_USER

This parameter enables auto-populating requester name on tickets.

Title	Description
Parameter Name	DEFAULT_REQUESTER_TO_LOGGED_IN_USER
Parameter Description	If this parameter value is set to "Yes", when a new ticket form is opened the logged in user's name is automatically filled into the Requester Name field of the ticket. Other related fields like Phone, Email, etc. also get automatically updated. This is not applicable to Tickets created using Ticket Templates. If the value is set to "No" the user will have to manually update Contact Name in the Requester field every time as it is a required field.
Default Value	No
Valid Value	Yes / No
Impact Area	All Tickets Requester Field
Appears on Interface	Agents and Self-Service User

EMAIL_DELEGATE_TEXT_FOR_SELF_SERVICE_USERS

This parameter controls text in the 'from' field of a mail from Self-Service Users.

Title	Description
Parameter Name	EMAIL_DELEGATE_TEXT_FOR_SELF_SERVICE_USERS
Parameter Description	This parameter sets the delegate text that appears in the 'From' field of the email messages sent by SSU. This lets the user know

	which SSU or Group has sent the message, although the email has been sent out by Nimsoft Service Desk application. Allowed formats are: \$(sender_name) Routed Via or \$(sender_primary_group) Routed Via. If the value is set to Group instead of sender, the Group Name will be displayed
Default Value	Blank
Valid Value	Text in above format
Impact Area	Outgoing Email Messages
Appears on Interface	Agents and SSU

EMAIL_DELEGATE_TEXT_FOR_AGENTS

This parameter controls the text in the 'from' field of a mail from Service Desk Agents.

Title	Description
Parameter Name	EMAIL_DELEGATE_TEXT_FOR_AGENTS
Parameter Description	Sets the delegate text that will appear in the 'From' field of the email messages sent by service desk agents. This informs the recipient that though the Email has been sent out by Nimsoft Service Desk application, which Service Desk Agent or Support group the mail has originated from. Allowed formats: \$(sender_name) On Behalf Of or \$(sender_primary_group) On Behalf Of.
Default Value	Blank
Valid Value	Text
Impact Area	Outgoing Email Message
Appears on Interface	Agents and SSU

ALLOW_EMAIL_DELIVERY_ON_WORKLOG_ENTRY

This parameter manages the availability to use Send as Mail option for worklogs.

Title	Description

Parameter Name	ALLOW_EMAIL_DELIVERY_ON_WORKLOG_ENTRY
Parameter Description	If the parameter value is set to "Yes" , it allows Agents to send worklog updates as emails to intended recipients. A Send as Email Option is displayed in the Worklog Section of the tickets in the General Information Tab or the Worklog update from the Activity Tab of the tickets. By Checking Send as Email checkbox before saving the Worklog update, the agent can send the Worklog as an email using a system defined communication template. If the parameter value is set to 'No', the "Send as Email" option is hidden and the functionality is disabled.
Default Value	Yes
Valid Value	Yes / No
Impact Area	Worklog update Email from Tickets
Appears on Interface	Agents

HOME_TICKET_LIST_ROW_HIGHLIGHTING_CRITERIA

This parameter controls Highlighting of ticket list rows.

Title	Description
Parameter Name	HOME_TICKET_LIST_ROW_HIGHLIGHTING_CRITERIA
Parameter Description	This parameter controls the Ticket field value (such as Priority, Urgency, Impact, and Status), which will be used to determine the highlighting color for the entire row in the Home Page List Ticket Table. If the value is set to Disable Highlighting, all highlighting will be turned off. A user can select from the options made available by the administrator using this parameter as "Default". A user can also choose a personally preferred Highlighting criterion in "Update My Preferences" which will override the "Default" set up by administrator.
Default Value	Disable Highlighting
Valid Value	Select from Dropdown

Impact Area	Home Page Ticket Lists
Appears on Interface	Agents

HOME_TICKET_LIST_ENABLE_CONDITIONAL_ROW_HIGHLIGHTING

This parameter controls conditional highlighting of Rows in the Ticket Lists.

Title	Description
Parameter Name	HOME_TICKET_LIST_ENABLE_CONDITIONAL_ROW_HIGHLIGHTING
Parameter Description	Set the value to "Yes" to enable conditional row highlighting of a row in the Home page ticket list. In addition, select a row highlighting criteria such as Ticket Priority, Urgency, Impact or Status in the Slice Configuration Parameter HOME_TICKET_LIST_ROW_HIGHLIGHTING_CRITERIA. If the parameter value is set to "No" row highlighting is disabled and it over rides the row highlighting criteria values configured in Slice Configuration parameter HOME_TICKET_LIST_ROW_HIGHLIGHTING_CRITERIA.
Default Value	No
Valid Value	Yes / No
Impact Area	Home Page Ticket Lists
Appears on Interface	Agents

HOME_TICKET_LIST_ENABLE_SLA_STATUS_INDICATORS

This parameter controls display of SLA status flags in ticket lists.

Title	Description
Parameter Name	HOME_TICKET_LIST_ENABLE_SLA_STATUS_INDICATORS
Parameter Description	When the parameter value is "Yes" it displays SLA compliance status indicator flag icon for each row in the Home page Ticket List.

	The shade of the flag indicates a specific SLA compliance status as listed in "Show Legends" lookup for Ticket List. When the parameter value is set to "No", the SLA Compliance Status indicator flag is displayed in a light Gray shade for all tickets.
Default Value	No
Valid Value	Yes / No
Impact Area	Home Page, Ticket Lists
Appears on Interface	Agents

LOCK_TICKET_DURING_APPROVAL

This parameter enables locking of a ticket submitted for approval.

Title	Description
Parameter Name	LOCK_TICKET_DURING_APPROVAL
Parameter Description	If parameter value is set to "Yes", it locks the Ticket once the ticket is submitted for Approval. The ticket cannot be edited till the Approval process is completed; resulting in either Approval or Rejection. But a worklog can be added to a locked ticket. If the parameter value is set to "No", the Ticket remains editable during the Approval process. However, if the ticket is modified during the process, a Notification is sent informing all stake holders that the Ticket has been modified.
Default Value	Yes
Valid Value	Yes / No
Impact Area	Ticket Approval Workflow
Appears on Interface	Agents

OMIT_INLINE_ATTACHMENT_SIZE_LIMIT

This parameter controls uploading of very small files being delivered via email attachments.

Title	Description
Parameter Name	OMIT_INLINE_ATTACHMENT_SIZE_LIMIT

Parameter Description	This parameter is used to exclude uploading of files of small size (routinely attached and having no significance) when an email containing an inline / embedded attachment is sent to ticket. The default Value is 500 bytes. Files below 500 bytes will not be uploaded as attachment to the Ticket. Set appropriate value.
Default Value	500
Valid Value	Positive Integer
Impact Area	Incoming Emails for Tickets
Appears on Interface	Not Visible on GUI

ALLOW_RELATIONSHIP_WITH_CLOSED_TICKETS

This parameter manages the ability to relate an Open Ticket to a Closed Ticket.

Title	Description
Parameter Name	ALLOW_RELATIONSHIP_WITH_CLOSED_TICKETS
Parameter Description	This parameter can be used to allow relating of an Open Ticket to a Closed Ticket. If the parameter value is set to "True", users can now relate open ticket to a closed ticket. Set the value to "False" disables this feature.
Default Value	False
Valid Value	True/False
Impact Area	Related Tickets
Appears on Interface	Agents

ENABLE_GROUPING_OF_CUSTOM_FIELDS_INTO_SECTIONS

This parameter manages grouping of Custom Fields using section headers.

Title	Description
Parameter Name	ENABLE_GROUPING_OF_CUSTOM_FIELDS_INTO_SECTIONS
Parameter	The parameter controls how custom fields will appear in the

Description	Additional Information Tab (visual layout), their logical groupings, and how they will be enclosed within separate sections. Set the parameter value to 'True' to enable grouping of Custom Fields into section using section headers. Setting the value to "False" disables this feature.
Default Value	False
Valid Value	Ture/False
Impact Area	Tickets Additional Information Tab
Appears on Interface	Agents and SSU

Change Management

The following Slice Configuration Parameters are applicable to the Change Management process in the application. They are classified under Parameter Category "Change Management" in the Manage Slice Configuration form.

SHOW_REQUESTED_FOR_TAB_ON_CHANGE

This parameter controls the display of the "Requested on Behalf of" tab in Change Tickets.

Title	Description
Parameter Name	SHOW_REQUESTED_FOR_TAB_ON_CHANGE
Parameter Description	If this parameter value is set to "Yes", the "Requested On Behalf Of" Tab on a Change Ticket will be displayed. All details like "Requested on Behalf of" Contact Name, Organization, Phone Number, etc. will be displayed in the tab. Setting the parameter value to "No" hides the tab.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Change Ticket- Requested for Tab
Appears on Interface	Agents

NOTIFICATION_INTERVAL_FOR_APPROVED_CHANGES_NOT_COMPLETED

This parameter sets the reminder period for Approved Changes that have not been implemented.

Title	Description
Parameter Name	NOTIFICATION_INTERVAL_FOR_APPROVED_CHANGES_NOT_COMPLETED
Parameter Description	Sets the Time Interval (in Hrs.) to be kept between notifications sent to Assigned Group or Assigned Individual for Approved Change Requests that have not been completed as planned. A notification will be sent as an alert to the Assigned Group and Assigned Individual about the pending change, when the set time interval has elapsed after the Planned End Date of a change implementation.
Default Value	24 hours
Valid Value	Number (time in hours)
Impact Area	Change Approval Process Communications
Appears on Interface	Not visible on GUI

TIME_BEFORE_OUTSTANDING_CHANGE_REQUEST_APPROVAL_CHECK

This parameter controls the 'Pending Approval Reminder' notification for a planned change.

Title	Description
Parameter Name	TIME_BEFORE_OUTSTANDING_CHANGE_REQUEST_APPROVAL_CHECK
Parameter Description	Set a time interval (number of hours prior to planned Start Date / Time) of Change Request, to send reminder notification to Approvers for pending approvals. A reminder notification will be sent out at the set duration, as an alert to Approvers with Outstanding Approvals. Approvers

	will be notified about outstanding approvals at the set duration prior to the Planned Start Date for the Change.
Default Value	2 hours
Valid Value	Number (time value)
Impact Area	Change Approval process communications
Appears on Interface	Not visible on GUI

NOTIFICATION_INTERVAL_FOR_OUTSTANDING_APPROVAL_REMINDERS

This parameter controls the interval at which “Outstanding Approval Reminders” will be sent.

Title	Description
Parameter Name	NOTIFICATION_INTERVAL_FOR_OUTSTANDING_APPROVAL_REMINDERS
Parameter Description	Set the Time Interval (in Hrs.) between successive reminder notifications to Approvers for “outstanding approvals”. Reminder Notifications will be sent out to the Approver(s) at the set interval till the approver attends to the “Outstanding Approval”.
Default Value	24 hours
Valid Value	Number (time value)
Impact Area	Change Approval process communication
Appears on Interface	Not visible on GUI

CHG_INITIAL_STATUS

This parameter manages the Status field on a new Change Request.

Title	Description
Parameter Name	CHANGE_INITIAL_STATUS
Parameter	This parameter sets the initial status for a new Change Request.

Description	When a new Change Request is saved for the first time, the Value for the “Status” field is automatically set to the Default value set in this parameter or a value specified by the Administrator.
Default Value	New
Valid Value	Dropdown Options
Impact Area	Ticket Lifecycle workflow
Appears on Interface	Agent

CHANGE_INITIAL_REASON_CODE

This parameter manages the Reason Code field on a new Change Request.

Title	Description
Parameter Name	CHANGE_INITIAL_REASON_CODE
Parameter Description	This parameter sets the initial Reason Code for a new Change Request. When a new Change Request is saved for the first time, the Value for the “Reason Code” field is automatically set to the Default value set in this parameter or a value specified by the Administrator.
Default Value	Blank
Valid Value	Text
Impact Area	Ticket Lifecycle workflow
Appears on Interface	Agent

CHANGE_INITIAL_PHASE

This parameter manages the Phase field on a new Change Request.

Title	Description
Parameter Name	CHANGE_INITIAL_PHASE
Parameter	This parameter sets the initial Phase for a new Change Request.

Description	When a new Change Request is saved for the first time, the Value for the “Phase” field is automatically set to the Default value set in this parameter or a value specified by the Administrator.
Default Value	Blank
Valid Value	Text
Impact Area	Ticket lifecycle workflow
Appears on Interface	Agent

CHG_DISABLE_USER_EDITING_TICKET_STATUS

This parameter controls ability of agents to edit change tickets in specified statuses.

Title	Description
Parameter Name	CHG_DISABLE_USER_EDITING_TICKET_STATUS
Parameter Description	Set values of Status at which to restrict “editing of a Change Request”. Any Change Requests in the Default specified statuses or status specified by the administrator in this parameter cannot be “edited” by any user. The ticket can be accessed in Read Only mode.
Default Value	Resolved and Closed
Valid Value	Text from lookup options
Impact Area	Change Request updates
Appears on Interface	Agents and SSU

CHG_REQUESTER_REPLY_STATUS

This parameter manages the Status that gets applied when as Requester replies to or updates a change ticket.

Title	Description

Parameter Name	CHG_REQUESTER_REPLY_STATUS
Parameter Description	This parameter defines the Status value to be set on the Change Request when an email response is received from ticket's Requester/ Requested For contact or it is manually updated by a self-service user. It enables the Administrator to specify a status (for example, "Queued") to automatically update the Status of the Change Request, based on Email interaction with Requester / Requested For or manual update by Self Service User.
Default Value	Blank
Valid Value	Text (dropdown options)
Impact Area	Change Ticket – Status field
Appears on Interface	Agents

CHG_REQUESTER_REPLY_REASON_CODE

This parameter manages the Reason Code that gets applied when a Requester replies to or updates a change ticket.

Title	Description
Parameter Name	CHG_REQUESTER_REPLY_REASON_CODE
Parameter Description	This parameter defines the Reason Code to be set on the Change Request when an Email response is received from ticket's Requester/ Requested For contact or it is manually updated by an SSU. It enables the Administrator to provide a text (for example, "Responded by User") to be automatically populated in the Reason Code field of the Change Request, to indicate Email interaction with Requester / Requested For or manual update by SSU.
Default Value	Blank
Valid Value	Text
Impact Area	Change ticket - reason code field

Appears on Interface	Agents

CHG_DISABLE_USER_EDITING_AFFECTED_CI_AND_LOCATIONS

This parameter controls locking of the Affected CI and Affected Location fields on a Change ticket.

Title	Description
Parameter Name	CHG_DISABLE_USER_EDITING_AFFECTED_CI_AND_LOCATIONS
Parameter Description	If the parameter value is set to “Yes”, it does not allow users to edit the values for Affected Configuration Items (CI) and Affected Locations in the More Detailed Information tab of Change. When the Value is set to “No”, it allows the users accessing the ticket to edit these two fields. An exception is when Tickets is locked during Approval and made Read Only. If set to “Yes”, the values in the two fields will be “Read Only” once the ticket record is saved.
Default Value	No
Valid Value	Yes/No
Impact Area	Change Ticket – Additional Information Tab
Appears on Interface	Agents

CHG_ENABLE_CUSTOM_FIELDS

This parameter controls the ability to display custom fields on change tickets.

Title	Description
Parameter Name	CHG_ENABLE_CUSTOM_FIELDS
Parameter Description	If parameter is set to “Yes”, the Additional Information tab on the Change Request, along with “Custom Fields” associated to the Change Ticket gets displayed. Setting the parameter value to “No” hides the Additional Information tab disables the ability to capture information for

	Custom Fields on a Change Ticket.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Change Ticket- Additional Information Tab
Appears on Interface	Agents

CHG_INITIAL_PRIORITY

This parameter sets the default Priority value for change tickets.

Title	Description
Parameter Name	CHG_INITIAL_PRIORITY
Parameter Description	Set the “Default Priority” for a new Change Request. The System Default is Medium (Code 3), which represents the most common value users may assign and requires user to change it only if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Priority field. Administrator can specify any other valid Priority value based on the needs of the User organization.
Default Value	Medium
Valid Value	Dropdown Options
Impact Area	Change Ticket- Priority field
Appears on Interface	Agents

CHG_INITIAL_SOURCE

This parameter sets the default Source value for change tickets.

Title	Description
Parameter Name	CHG_INITIAL_SOURCE
Parameter Description	Set the default value for “Source” for a new Change Request. System Default is Web (Code 4). The Default initial “Source” represents the most common mode of user’s interaction with

	Service Desk. It requires Agent User to change the value only if necessary for a specific ticket. Administrator can specify any other valid value for Source field based on the most common mode of interaction for the User organization.
Default Value	Web
Valid Value	Dropdown options
Impact Area	Change Ticket- Source field
Appears on Interface	Agents

CHG_INITIAL_URGENCY

This parameter sets the default value for Urgency on new change tickets.

Title	Description
Parameter Name	CHG_INITIAL_URGENCY
Parameter Description	Set the default value for “Urgency” for a new Change Request. System Default is medium (Code 2). The default initial value for Urgency represents the most common value users may assign and requires user to change it only if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” urgency field. The Administrator can specify any other valid “Urgency” value based on the needs of the User organization.
Default Value	Medium
Valid Value	Dropdown options
Impact Area	Change Ticket- Urgency field
Appears on Interface	Agents

CHG_INITIAL_IMPACT

This parameter sets the default value for Impact for a new change ticket.

Title	Description
Parameter Name	CHG_INITIAL_IMPACT
Parameter Description	Set the default value for Impact for a new Change Request. System Default is medium (Code 2). The default initial value for Impact represents the most common value users may assign and requires user to change it only if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Impact field. The Administrator can specify any other valid Impact value based on the needs of the User organization.
Default Value	Medium
Valid Value	Dropdown Options
Impact Area	Change Ticket- Impact field
Appears on Interface	Agents

CHANGE_ENABLE_APPROVAL_ROUTING

This parameter manages setting up of Multi-Level Approval and Approval Routing workflow.

Title	Description
Parameter Name	CHANGE_APPROVAL_ROUTING
Parameter Description	Setting the value to “Yes”, enables configuring multi-tiered “Approval Routing Workflow” processes for Change Requests. When enabled, the Change Request shall display the Approval tab with the relevant details such as Approval Phase, Names of Approvers/ Reviewers, Status of Approval Decisions by them, etc.

	In addition, Workflow Actions configured by Administrator for Submitting Change Requests for Approval and Withdrawing Change from Approval can be accessed in “Take an Action” Menu for the ticket. Notification and Reminders related to the Approval process shall be sent to Approvers / Reviewers and other participants as per workflow configured. Approvers / Reviewers shall be able to view “My Outstanding Approvals” information and interact to record their decisions. Set the parameter value to “No” to disable and Hide all the above Approval related functions and features.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Change Approval Process
Appears on Interface	Agents and Admin

CHANGE_WORKLOG_REQUIRED_FIELD_LIST

This parameter controls which fields on the change Worklog section are marked as “Required field” before a change ticket is saved.

Title	Description
Parameter Name	CHANGE_WORKLOG_REQUIRED_FIELD_LIST
Parameter Description	Set the worklog fields which you would like to mark as “Required Fields” when adding a worklog for Change Tickets. The fields specified as mandatory will require the user to provide a value compulsorily. If the value is not available, a message asking the user to provide the value before saving the Ticket record.
Default Value	Blank
Valid Value	Available Checkbox options
Impact Area	Change Ticket- Worklog fields
Appears on Interface	Agents

CHANGE_DEFAULT_ASSIGNMENT_GROUP

This parameter controls the display of the "Requested on Behalf of" tab in Change Tickets.

Title	Description
Parameter Name	CHANGE_DEFAULT_ASSIGNMENT_GROUP
Parameter Description	Set the default Support Group to which incoming Change Requests get assigned, when no assignment rules get executed. The Change Request gets assigned to the identified group, the Assigned To Group field gets set and the Status is set to the default initial status. The Change Ticket is then visible to the members of the Assigned Group in the Ticket List (Change Request List and Ticket List under Home). The Administrator can specify any Support Group ID to which all new Change Request get assigned for processing.
Default Value	1
Valid Value	Group ID
Impact Area	Change Ticket- Assigned Group field
Appears on Interface	Agents

Configuration Management

The following Slice Configuration Parameters are applicable to Configuration Management in the application. They are classified under Parameter Category "Configuration Management" in the Manage Slice Configuration form

SCR_AFFECTED_SERVICES_SEARCH_DEPTH

This parameter controls the depth to which Related CIs will be traversed in a CI Hierarchy.

Title	Description
Parameter Name	SCR_AFFECTED_SERVICES_SEARCH_DEPTH
Parameter Description	Set the number of higher parent levels to be traversed in Configuration Items hierarchy to include Services supported by related CIs of a Ticket, in the Affected Service Lookup for the

	Ticket. When the value is set to “0”, the entire relationship hierarchy above the related CI as Parent, Grand Parent, Great Grand Parents, etc. shall be traversed. All Services supported by the higher CIs shall be included in Affected Services Lookup. Specify an inter value to limit the number of levels to be traversed. The same parameter also controls the Depth of the relationships to be displayed in the Relationship graph for a CI.
Default Value	0
Valid Value	Zero or positive integer
Impact Area	Tickets – Affected services lookup or Configuration Management – CI Relationship graph
Appears on Interface	Agents

Incident Management

The following Slice Configuration Parameters control features related to Incident Management in the application. They are classified under Parameter Category “Incident Management” in the Manage Slice Configuration form.

INC_INITIAL_STATUS

This parameter controls the “initial status” on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_STATUS
Parameter Description	Set the “initial status” for a new Incident Ticket. The System Default value is New. The administrator can choose an alternate valid value. When a new Incident Ticket is saved for the first time, the value for the Status field is automatically set to a Default value set by the Administrator.
Default Value	New
Valid Value	Dropdown Options

Impact Area	Ticket Lifecycle workflow – Status
Appears on Interface	Agents and SSU

INC_INITIAL_REASON_CODE

This parameter controls the “Initial Reason Code” on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_REASON_CODE
Parameter Description	Set the Initial Reason Code” value for a new Incident Ticket, when the ticket is first saved. The System Default value is “Identified”. The administrator can set any alternate valid value. When a new Incident Ticket is saved for the first time, the value for the Reason Code field is automatically set to the Default value set by the Administrator.
Default Value	Identified
Valid Value	Text
Impact Area	Ticket Lifecycle workflow – Reason Code
Appears on Interface	Agents and SSU

INC_INITIAL_PHASE

This parameter controls the “initial Phase” on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_PHASE
Parameter Description	Set the “Initial Phase” for a new Incident Ticket. The System Default is “Initial Diagnosis”. The administrator can define any alternate valid value.

	When a new Incident Ticket is saved first time, the value for the Phase field is automatically set to the default value defined by the Administrator.
Default Value	Initial Diagnosis
Valid Value	Text
Impact Area	Ticket Lifecycle workflow – Phase
Appears on Interface	Agents and SSU

INC_DISABLE_USER_EDITING_TICKET_STATUS

This parameter controls the ability of user to edit Incident Ticket in identified statuses.

Title	Description
Parameter Name	INC_DISABLE_EDITING_TICKET_STATUS
Parameter Description	Set the status to restrict user “editing of Incident Ticket”. The System Default values are Resolved or Closed. Incident Ticket in any of the specified status cannot be edited by any user and can be accessed in Read Only mode.
Default Value	Resolved and Closed
Valid Value	Text from Dropdown list
Impact Area	Incident Ticket Updates
Appears on Interface	Agents and SSU

INC_REQUESTER_REPLY_STATUS

This parameter controls the status updated when a requester replies to an incident ticket.

Title	Description
Parameter Name	INC_REQUESTER_REPLY_STATUS

Parameter Description	This parameter defines the Status value to be set on the Incident Ticket when an email response is received from ticket's Requester/ Requested For contact or it is manually updated by an SSU. Default is Blank (no value). Valid values are Ticket Status values. It enables the Administrator to specify a status (for example, "Queued") to automatically update the status of the Incident Ticket, based on Email interaction with Requester / Requested For or manual update by SSU.
Default Value	Blank
Valid Value	Text (dropdown list)
Impact Area	Incident Ticket Status
Appears on Interface	Agents

INC_REQUESTER_REPLY_REASON_CODE

This parameter sets the Reason Code on an Incident Ticket updated by requester response.

Title	Description
Parameter Name	INC_REQUESTER_REPLY_REASON_CODE
Parameter Description	Set the "Reason Code" to be displayed on the Incident Ticket when an email response is received from ticket's Requester/ Requested For contact or it is manually updated by an SSU. Default is Blank (No Value). This enables the Administrator to provide a text (for example, "Responded by User") to be automatically populated in the Reason Code field of the Incident Ticket to indicate Email interaction with Requester / Requested For or manual update by SSU.
Default Value	Blank
Valid Value	Text
INC_INITIAL_STATUS	
Impact Area	This parameter controls the "initial status" on a new Incident Ticket.
Appears on Interface	Agents

INC_ENABLE_CUSTOM_FIELDS

This parameter manages the display of Custom Fields on Incident Tickets.

Title	Description
Parameter Name	INC_ENABLE_CUSTOM_FIELDS
Parameter Description	When the parameter value is set to “Yes”, the Additional Information tab is displayed on the Incident Tickets, with the “Customs Fields associated with the Ticket”. Custom Fields allow tracking information in addition to the standard fields for Incident Tickets. Setting the value to “No” hides the Additional Information tab and disables the ability to capture information from the Customs Fields.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Incident Ticket-Additional Information Tab
Appears on Interface	Agents and SSU

INC_DEFAULT_ASSIGNMENT_GROUP

This parameter identifies the support group to which Incident Tickets get assigned by default.

Title	Description
Parameter Name	INC_DEFAULT_ASSIGNMENT_GROUP
Parameter Description	Specify the default Support Group to which incoming Incident Ticket get assigned when no assignment rules get executed. The System Default Value is 1 (Administration Group). The Incident Ticket gets assigned to the specified group by default, and the Assigned to Group name is set in the Assigned to field; with the Status value set as Default Initial Status. The ticket is visible to the members of the Assigned Group in the Ticket List (Incident ticket List and Ticket List under Home).The Administrator can specify the ID for any Support Group to which all new Incident Tickets get assigned for processing.

Default Value	1
Valid Value	Group ID
Impact Area	Incident Ticket Assigned to Group field
Appears on Interface	Agents and SSU

INC_MATCH_INCIDENT_ON_CREATE_USING_XML

This parameter manages relating of an email received to open Incident Tickets.

Title	Description
Parameter Name	INC_MATCH_INCIDENT_ON_CREATE_USING_XML
Parameter Description	If the parameter value is set to “Yes”, the description field of incoming Email XML is compared with the descriptions of Open Incident tickets. If a match is found, the email XML modifies the matching open incident ticket instead of creating a new Incident ticket. If the value is set to “No”, a new Incident Ticket is created using incoming Email XML.
Default Value	Yes
Valid Value	Yes\No
Impact Area	Incident ticket creating using Email
Appears on Interface	Not Visible on GUI

INC_INITIAL_PRIORITY

This parameter controls the “initial Priority” value on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_PRIORITY
Parameter Description	Set the initial Priority for a new Incident Ticket. The System Default is Medium (Code 3). You can specify any alternate value from available options. The default initial value of Priority represents the most common value users may assign. Users can change it if necessary for a specific ticket. A default initial value also ensures proper functioning of processes which cannot accept a “Blank” Priority field. All new Incident tickets will carry the default Priority Value defined.
Default Value	Medium
Valid Value	Text from Dropdown
Impact Area	Incident Ticket – Priority field
Appears on Interface	Agent and SSU

INC_INITIAL_SOURCE

This parameter controls the “initial Source” value on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_SOURCE
Parameter Description	Sets the initial “Source” for a new Incident Ticket. The System Default is Web (Code 4). You can set any alternate value from the available options. The default Initial Source represents the most common mode of user’s interaction with Service Desk. An agent can change the value if necessary for a specific ticket. All new Incident tickets will carry the default Source Value defined.

Default Value	Web
Valid Value	Text from Dropdown
Impact Area	Incident Ticket – Source field
Appears on Interface	Agent and SSU

INC_INITIAL_URGENCY

This parameter controls the “initial Urgency” value on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_URGENCY
Parameter Description	Sets the initial “Urgency” for a new Incident Ticket. The system default is Medium (Code 2). You can set any alternate value from the available options. The default initial value of Urgency represents the most common value users may assign. A user can change it if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” urgency field. All new Incident tickets will carry the default Source Value defined.
Default Value	Web
Valid Value	Text from Dropdown
Impact Area	Incident Ticket – Urgency field
Appears on Interface	Agent and SSU

INC_INITIAL_IMPACT

This parameter controls the “Impact” value on a new Incident Ticket.

Title	Description
Parameter Name	INC_INITIAL_IMPACT
Parameter	Sets the initial “Urgency” for a new Incident Ticket. The system

Description	default is Medium (Code 2). You can set any alternate value from the available options. The default initial value of Urgency represents the most common value users may assign. A user can change it if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” urgency field. All new Incident tickets will carry the default Source Value defined.
Default Value	Medium
Valid Value	Text from Dropdown
Impact Area	Incident Ticket – Impact field
Appears on Interface	Agent and SSU

INC_ENABLE_APPROVAL_ROUTING

This parameter is currently inoperative. It manages “approval routing” for Incident Tickets.

Title	Description
Parameter Name	INC_ENABLE_APPROVAL_ROUTING
Parameter Description	When the parameter value is set to “Yes”, multi-tiered “approval routing” workflow processes for Incident Ticket gets enabled. When enabled, the Incident Ticket displays the Approval Tab with the relevant details such as Approval Phase, Names of Approvers/ Reviewers, status of Approval Decisions by them, etc. In addition, Workflow actions configured by Administrator for Submitting Incident Ticket for Approval and Withdrawing them from Approval can be accessed in “Take an Action” menu for the ticket. Notification and Reminders related to Approval process shall be sent to Approvers / Reviewers and other participants as per workflow configured. Approvers / Reviewers shall be able to view “My Outstanding Approvals” information and interact to record their decisions. Set the parameter value to “No” to disable Approval Routing for incident tickets and hide all the above Approval related

	functions and features.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Incident Ticket – Approval Process
Appears on Interface	Agent and Admin

WORKLOG_REQUIRED_FIELDS_LIST

This parameter manages the fields in the worklog section which are to be marked as Required Fields.

Title	Description
Parameter Name	WORKLOG_REQUIRED_FIELDS_LIST
Parameter Description	Set the worklog fields which you would like to mark as required fields when adding a worklog for Incident Tickets. The fields specified as mandatory will require the user to provide a value compulsorily. If the value is not available, a message asking the user to provide the value before saving the Ticket record is displayed.
Default Value	All boxes unchecked
Valid Value	Checkbox options
Impact Area	Incident Ticket – Worklog fields
Appears on Interface	Agent

Knowledge Management

The Slice Configuration Parameters listed below control functionality related to Knowledge Management. They are classified under the Parameter Category “Knowledge Management” in the Manage Slice Configuration form.

KB_ARTICLE_SEARCH_INCLUDE_TICKETS_RESOLVED_WITHIN_PERIOD

This parameter manages the ability to use recently resolved tickets to find solution for open tickets.

Title	Description
Parameter Name	KB_ARTICLE_SEARCH_INCLUDE_TICKETS_RESOLVED_WITHIN_PERIOD
Parameter Description	Set time period of resolved tickets that can be included in a search for solutions recorded on resolved tickets. This will allow agents to extend their search for solutions from a ticket, to include older ticket solutions which may not yet have been formalized as approved Knowledge Articles in Knowledge Management. The system default is ‘None’. Choose an alternate value to allow recently resolved tickets to be searched and used to resolve open tickets.
Default Value	None
Valid Value	Radio button Options
Impact Area	Search Solutions
Appears on Interface	Agent

ENABLE_KEYWORD_BASED_KB_SEARCH

This parameter manages the Initial Source for tickets created via email conversions.

Title	Description
Parameter Name	ENABLE_KEYWORD_BASED_KB_SEARCH
Parameter Description	Set the appropriate parameter value to enable or disable Keyword based Search through the knowledgebase. If the value is set to yes, Keyword based search is enabled. If set to no, the search mechanism switches to java based full text search.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Global Search for KB Article, Search Solutions via keywords generation, Knowledge based ticket search.
Appears on Interface	All Users

Note: Keyword based search could result in unexpected results for articles and solutions that are not in English. If majority of the items stored and accessed will be in a language other than English, it is recommended that you set this parameter value to NO, and thereby set Full Text Search as the more effective search mechanism

Problem Management

The Slice Configuration Parameters listed below control functionality related to Problem Management. They are classified under the Parameter Category “Problem Management” in the Manage Slice Configuration form.

VIEW_SEVERITY_ON_PROBLEM

This parameter controls the display of “Severity Field” on Problem Tickets.

Title	Description
Parameter Name	VIEW_SEVERITY_ON_PROBLEM
Parameter Description	To display the “Severity Field” on the General Information tab of Problem Tickets, set parameter value to “Yes”. When the value is set to “No”, the “Severity Field” is hidden.

	However, even when hidden, the “Severity Field” has a default value “Normal”. All other workflows will function as if the Value of the “Severity Field” is “Normal”.
Default Value	Yes
Valid Value	Yes\No
Impact Area	Problem Ticket _Severity field
Appears on Interface	Agent

SHOW_AFFECTED_USERS_TAB_ON_PROBLEM

This parameter controls display of “Affected Users Tab” on Problem Tickets.

Title	Description
Parameter Name	SHOW_AFFECTED_USERS_TAB_ON_PROBLEM
Parameter Description	This parameter manages the display of “Who is having the Issue” Tab in the Agent’s view of Problem tickets. Set the value as “Yes” to display the tab with Name, Phone Number, Email, Organization, Site and Location information of the contact who is having the Issue. Select “No” to hide the tab.
Default Value	Yes
Valid Value	Yes\No
Impact Area	Problem Ticket _Who’s having the issue tab
Appears on Interface	Agent

PRB_INITIAL_STATUS

This parameter manages the default value for “Status of New Problem Tickets”.

Title	Description
Parameter Name	PRB_INITIAL_STATUS
Parameter	Set a default value to be assigned to the “Status” field of a

Description	Problem Ticket when it is first saved. The system default value is "New".
PRB_INITIAL_REASON_CODE	Set an alternate value from available options. When a new Problem Ticket is saved for the first time, the value for the Status field is automatically set to the default value set by the Administrator.
Default Value	New
Valid Value	Text From Dropdown options
Impact Area	Problem Ticket Status field
Appears on Interface	Agent

This parameter controls the Reason Code value displayed on new Problem Tickets.

Title	Description
Parameter Name	PRB_INITIAL_REASON_CODE
Parameter Description	Set a default value to be assigned to the "Reason Code" field of a Problem Ticket when it is first saved. The system default value is "None". Set an alternate value as appropriate. When a new Problem Ticket is saved for the first time, the value for the "Reason Code" field is automatically set to the default value set by the Administrator.
Default Value	None
Valid Value	Text
Impact Area	Problem Ticket Reason Code field
Appears on Interface	Agent

PRB_INITIAL_PHASE

This parameter controls the value displayed in the Phase field of Problem Tickets.

Title	Description
Parameter Name	PRB_INITIAL_PHASE

Parameter Description	Set a default value to be assigned to the “Phase” field of a Problem Ticket when it is first saved. The system default value is “Investigation”. Set an alternate value as appropriate. When a new Problem Ticket is saved for the first time, the value for the “Phase” field is automatically set to the default value set by the Administrator.
Default Value	Investigation
Valid Value	Text
Impact Area	Problem Ticket Phase field
Appears on Interface	Agent

PRB_DISABLE_USER_EDITING_TICKET_STATUS

This parameter controls the statuses at which a problem ticket cannot be edited.

Title	Description
Parameter Name	PRB_DISABLE_USER_EDITING_TICKET_STATUS
Parameter Description	This parameter sets the Status values which restrict Problem Ticket editing. The system default Values is Resolved, Closed. Problem Tickets in any of the specified status cannot be edited by any user and can be accessed in Read Only mode. Set alternate values from available options.
Default Value	Resolved/Closed
Valid Value	Text from dropdown options
Impact Area	Problem Ticket updates
Appears on Interface	Agent

PRB_REQUESTER_REPLY_STATUS

This parameter controls the Status updated when a requester replies to or updates a Problem Ticket.

Title	Description

Parameter Name	PRB_REQUESTER_REPLY_STATUS
Parameter Description	This parameter defines the Status value to be set on the Problem Ticket when an email response is received from ticket's Requester/ Affected User contact or it is manually updated by a Self-Service User. Default is Blank. Valid Values are Ticket Status values. It enables the Administrator to specify a status (for example, "Queued") to automatically update the Status of the Problem Ticket, based on Email interaction with Requester / Affected User or manual update by Self Service User.
Default Value	Blank
Valid Value	Text from dropdown options
Impact Area	Problem Ticket Status field
Appears on Interface	Agent

PRB_REQUESTER_REPLY_REASON_CODE

This parameter controls the "Reason Code" updated when a requester replies to or updates a Problem Ticket.

Title	Description
Parameter Name	PRB_REQUESTER_REPLY_REASON_CODE
Parameter Description	This parameter defines the "Reason Code" to be set on the Problem ticket when an email response is received from ticket's Requester/ Requested For contact or it is manually updated by an SSU. Default is "No Value". It enables the Administrator to provide a text (for example, "Responded by User") to be automatically populated in the "Reason Code" field of the Problem ticket to indicate Email interaction with Requester / Requested For or manual update by SSU.
Default Value	Blank
Valid Value	Text
Impact Area	Problem Ticket Reason Code field

Appears on Interface	Agent

PRB_ENABLE_CUSTOM_FIELDS

This parameter controls the ability to add “Custom Fields” to Problem Tickets.

Title	Description
Parameter Name	PRB_ENABLE_CUSTOM_FIELDS
Parameter Description	When the parameter value is set to “Yes”, “Custom Fields” associated with the ticket are displayed in Additional Information tab of Problem Tickets. “Custom Fields” allow tracking information in addition to the standard fields for Problem Ticket. Selecting parameter value “No” hides the Additional Information tab “Custom Fields” will not be displayed on Problem Tickets.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Problem Ticket Additional Information Tab
Appears on Interface	Agent

PRB_INITIAL_PRIORITY

This parameter controls the default “Priority” field value for a new Problem Ticket.

Title	Description
Parameter Name	PRB_INITIAL_PRIORITY
Parameter Description	Sets the initial value ‘Priority’ field for a new Problem Ticket. The system default is Medium (Code 3). You can choose an alternate value from the available options. The default initial

	value for “Priority” represents the most common value users may assign. Users can change it if necessary for a specific ticket. Setting a Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Priority field. All new Problem Tickets logged will carry the default “Priority” field value.
Default Value	Medium
Valid Value	Text from Dropdown options
Impact Area	Problem Ticket Priority field
Appears on Interface	Agent

PRB_INITIAL_SOURCE

This parameter sets the default value for “Source” of a Problem Ticket.

Title	Description
Parameter Name	PRB_INITIAL_SOURCE
Parameter Description	Sets the initial value for the ‘Source’ field for a new Problem Ticket. The system default is Web (Code 4). You can specify any alternate value from available options. The default initial value for Source represents the most common mode of user’s interaction with Service Desk. Users can change the value if necessary for a specific ticket. All new Problem Tickets logged will carry the default Priority field value.
Default Value	Web
Valid Value	Text from Dropdown options
Impact Area	Problem Ticket Source field
Appears on Interface	Agent

PRB_INITIAL_URGENCY

This parameter controls the default “Urgency” field value for a new Problem Ticket.

Title	Description

Parameter Name	PRB_INITIAL_URGENCY
Parameter Description	Sets the initial value for “Urgency” field for a new Problem Ticket. The system default is Medium (Code 2). You can choose any alternate value from the available options. The default initial value for Urgency represents the most common value users may assign. Users can change it if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” urgency field. All new Problem Tickets logged will carry the default Urgency field value.
Default Value	Medium
Valid Value	Text from Dropdown options
Impact Area	Problem Ticket Urgency field
Appears on Interface	Agent

PRB_INITIAL_IMPACT

This parameter controls the default “Impact” field value for a new Problem Ticket.

Title	Description
Parameter Name	PRB_INITIAL_IMPACT
Parameter Description	This parameter sets the initial value for “Impact” for a new Problem Ticket. The system default is Medium (Code 2). You can choose an alternate value from the available options. The default initial value for Impact represents the most common value users may assign. Users can change it if necessary for a specific ticket. Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Impact field. All new Problem Tickets logged will carry the default Urgency field value.
Default Value	Medium
Valid Value	Text from Dropdown options
Impact Area	Problem Ticket Impact field

Appears on Interface	Agent

PRB_ENABLE_APPROVAL_ROUTING

This parameter is currently dysfunctional. It controls the ability to set up “Approval Routing” for Problem Tickets.

Title	Description
Parameter Name	PRB_ENABLE_APPROVAL_ROUTING
Parameter Description	When this parameter is set to “Yes”, it enables multi-tiered “Approval Routing” and workflow processes for Problem Tickets. When enabled, the Problem Ticket will display the Approval Tab with the relevant details such as Approval Phase, Names of Approvers/ Reviewers, status of Approval Decisions by them, etc. In addition, Workflow actions configured by Administrator for Submitting Incident Ticket for Approval and withdrawing them from Approval can be accessed in “Take an Action” menu for the ticket. Notification and Reminders related to Approval process shall be sent to Approvers / Reviewers and other participants as per workflow configured. Approvers / Reviewers shall be able to view “My Outstanding Approvals” information and interact to record their decisions. Setting the parameter value to “No” - will disable approval routing and hides all the above Approval related functions and features.
Default Value	No
Valid Value	Yes/No
Impact Area	Problem Ticket Approval Process
Appears on Interface	Agent

PRB_WORKLOG_REQUIRED_FIELDS_LIST

This parameter manages the fields in the worklog section which are to be marked as “Required Fields”.

Title	Description
Parameter Name	PRB_WORKLOG_REQUIRED_FIELDS_LIST
Parameter Description	Set the worklog field where you would like inputs to be mandatory when adding a worklog for Change Requests. The fields specified as mandatory shall require user to provide a value. If the value is not available, a message asking the user to provide the value before saving the Ticket record is displayed.
Default Value	All checkboxes unchecked
Valid Value	Checkbox options
Impact Area	Problem Ticket Worklog fields
Appears on Interface	Agent

PRB_DEFAULT_ASSIGNMENT_GROUP

This parameter controls the Default Group to which Problem Tickets get assigned.

Title	Description
Parameter Name	PRB_DEFAULT_ASSIGNMENT_GROUP
Parameter Description	This parameter defines the default Support Group to which incoming Problem Ticket must be assigned when no assignment rules get executed. The system default value is 1 (Administration Group). You can choose any alternate group to which problem tickets must be assigned to for processing. The Problem Ticket gets assigned to the default group, with Assigned to Group name displayed in Assigned to field.

	The Status and Reason Code are set to default Initial Status and Reason Code defined by the administrator.
Default Value	1
Valid Value	Group ID
Impact Area	Problem Ticket Assigned to Group field
Appears on Interface	Agent

Request Management

The Slice Configuration Parameters listed below control features related to Request Management. They are categorized under the Parameter Category “Request Management” in the Manage Slice Configuration form.

SRQ_INITIAL_STATUS

This parameter controls the default value for the Status field of New Service Request.

Title	Description
Parameter Name	SRQ_INITIAL_STATUS
Parameter Description	Set a default value to be assigned to the Status field of a Service Request when it is first saved. The system default value is “New”. Set an alternate value as appropriate. When a new Service Request is saved for the first time, the value for the Status field is automatically set to the default value set by the Administrator.
Default Value	New
Valid Value	Dropdown options
Impact Area	Ticket Lifecycle workflow- Status
Appears on Interface	Agent and SSU

SRQ_INITIAL_REASON_CODE

This parameter controls the default value for the Status field of New Service Request.

Title	Description
Parameter Name	SRQ_INITIAL_REASON_CODE
Parameter Description	Set a default value to be assigned to the Reason Code field of a Service Request when it is first saved. The system default value is “None”. Set an alternate value as appropriate. When a new Service Request is saved for the first time, the value for the Reason Code field is automatically set to the default value set by the Administrator.
Default Value	None
Valid Value	Text
Impact Area	Ticket Lifecycle workflow- Reason Code
Appears on Interface	Agent and SSU

SRQ_DEFAULT_ASSIGNMENT_GROUP

This parameter controls the “default assignment group” for New Service Request.

Title	Description
Parameter Name	SRQ_DEFAULT_ASSIGNMENT_GROUP
Parameter Description	Set the default Support Group to which incoming Service Requests get assigned when no assignment rule gets executed. The system default Value is 1 (Administration Group). The new Service Request gets assigned to the default group with Group Name displayed in Assigned to field. The Status and Reason Code of the new Service Request are set as default Initial Status and Initial Reason Code.
Default Value	1
Valid Value	Support Group ID
Impact Area	Service Request Assigned to Group field
Appears on Interface	Agent

SRQ_INITIAL_PHASE

This parameter controls the default value for the Phase field of New Service Request.

Title	Description
Parameter Name	SRQ_INITIAL_PHASE
Parameter Description	Set a default value to be assigned to the “Phase” field of a Service Request when it is first saved. The system default value is “Request Preparation”. Set an alternate value as appropriate. When a new Service Request is saved for the first time, the value for the Phase field is automatically set to the default value set by the Administrator.
Default Value	Validation
Valid Value	Text
Impact Area	Service Request Phase field
Appears on Interface	Agent

SRQ_DISABLE_USER_EDITING_TICKET_STATUS

This parameter controls the status at which a Service Request Ticket cannot be edited.

Title	Description
Parameter Name	SRQ_DISABLE_USER_EDITING_TICKET_STATUS
Parameter Description	This parameter sets the Status values which restrict edition o Service Request Tickets. The system default Values is Resolved, Closed. Problem Tickets in any of the specified status cannot be edited by any user and can be accessed in Read Only mode. Set alternate values from available options.
Default Value	Resolved and Closed
Valid Value	Text from dropdown options
Impact Area	Service Request Updates

Appears on Interface	Agent and SSU

SRQ_REQUESTER_REPLY_REASON_CODE

This parameter manages to “Reason Code” to be set when requester updates the Service Request.

Title	Description
Parameter Name	SRQ_REQUESTER_REPLY_REASON_CODE
Parameter Description	This defines the “Reason Code” to be set on the Service Request when an email response is received from ticket’s Requester/ Requested For contact or it is manually updated by a SSU. The Default is No Value. This enables the Administrator to provide a text (for example, “Responded by User”) to be automatically populated in the Reason Code field of the Service Request, to indicate Email interaction with Requester / Requested For or manual update by SSU.
Default Value	Blank
Valid Value	Text
Impact Area	Service Request Updates
Appears on Interface	Agent

SRQ_REQUESTER_REPLY_STATUS

This parameter manages to Status to be set when requester updates the Service Request.

Title	Description
Parameter Name	SRQ_REQUESTER_REPLY_STATUS
Parameter Description	This parameter defines the “Status” value to be set on the Service Request when an email response is received from ticket’s Requester/ Requested For contact or it is manually updated by a SSU. Default is Blank. Valid Values is same as the “Ticket Status” value. It enables the Administrator to specify a status (for example, “Queued”) to automatically update the Status of the Service Request, based on Email interaction with Requester / Requested For or manual update by Self-Service User.

Default Value	Blank
Valid Value	Text from dropdown
Impact Area	Service Request Status field
Appears on Interface	Agent and SSU

SRQ_ENABLE_CUSTOM_FIELDS

This parameter manages display of Custom Fields in the Additional Information Tab of Service Requests.

Title	Description
Parameter Name	SRQ_ENABLE_CUSTOM_FIELDS
Parameter Description	When the parameter value is set to “Yes”, the Additional Information tab is displayed on the Service Request, with the “Customs Fields” associated with the Ticket. “Custom Fields” allow tracking information in addition to the standard fields for Service Requests. Setting the value to “No” hides the Additional Information tab and disables the ability to capture information from the customs fields.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Service Request Additional Information Tab
Appears on Interface	Agent and SSU

SRQ_INITIAL_PRIORITY

This parameter manages the default value for “Service Request Priority field”.

Title	Description
Parameter Name	SRQ_INITIAL_PRIORITY
Parameter Description	This parameter sets the initial “Priority” for a new Service Request. The system default is Medium (Code 3). You can

	specify an alternate value from the available options. The default initial Priority represents the most common value users may assign. Users can change it if necessary for a specific ticket. Setting a Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Priority field. All new Service Requests will display the default priority value.
Default Value	Medium
Valid Value	Text from dropdown
Impact Area	Service Request Priority Field
Appears on Interface	Agent and SSU

SRQ_INITIAL_SOURCE

This parameter manages the default value for “Service Request Source field”

Title	Description
Parameter Name	SRQ_INITIAL_SOURCE
Parameter Description	This parameter sets the initial “Source” for a new Service Request. The system default is Web (Code 4). You can specify an alternate value from the available options. The default initial Source represents the most common value users may assign. Users can change it if necessary for a specific ticket. Setting a Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Source field. All new Service Requests will display the default Source value.
Default Value	Web
Valid Value	Text from dropdown
Impact Area	Service Request Source Field
Appears on Interface	Agent

SRQ_INITIAL_URGENCY

This parameter manages the default value for “Service Request Urgency field.”

Title	Description
Parameter Name	SRQ_INITIAL_URGENCY
Parameter Description	This parameter sets the initial “Urgency” for a new Service Request. The system default is Medium (Code 2). You can specify an alternate value from the available options. The default initial “Urgency” represents the most common value users may assign. Users can change it if necessary for a specific ticket. Setting a Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Urgency field. All new Service Requests will display the default Urgency value.
Default Value	Medium
Valid Value	Text from dropdown
Impact Area	Service Request Urgency Field
Appears on Interface	Agent

SRQ_INITIAL_IMPACT

This parameter manages the field value for “Service Request Impact field”.

Title	Description
Parameter Name	SRQ_INITIAL_IMPACT
Parameter Description	This parameter sets the initial “Impact” for a new Service Request. The system default is Medium (Code 2). You can specify an alternate value from the available options. The default initial Impact represents the most common value users may assign. Users can change it if necessary for a specific ticket. Setting a Default initial value also ensures proper functioning of processes which cannot accept a “Blank” Impact field. All new Service Requests will display the default Impact value.
Default Value	Medium

Valid Value	Text from dropdown
Impact Area	Service Request Urgency Field
Appears on Interface	Agent

SRQ_INITIAL_SOURCE_FOR_EMAIL_CONVERSIONS

This parameter manages the Initial Source for tickets created via email conversions.

Title	Description
Parameter Name	SRQ_INITIAL_SOURCE_FOR_EMAIL_CONVERSIONS
Parameter Description	This parameter sets the initial Source (origin) for a new Service Request created via conversion of incoming emails into Service Request. The system default is Email. You can use Advanced Search for tickets, where you can search using Source. Populating a specific value into tickets created via conversion of email enables easy search for these tickets.
Default Value	Email
Valid Value	Text from dropdown
Impact Area	Service Request Source Field
Appears on Interface	Agent

SRQ_ENABLE_APPROVAL_ROUTING

This parameter is currently inoperative. It manages approval routing for Service Requests.

Title	Description
Parameter Name	SRQ_ENABLE_APPROVAL_ROUTING
Parameter Description	If the value for this parameter is set to “Yes” it enables multi-tiered approval routing workflow processes for Service Requests. When enabled, the Service Request will display the Approval Tab with the relevant details such as Approval Phase, Names of Approvers/ Reviewers, status of Approval Decisions by them, etc.

	In addition, Workflow actions configured by Administrator for Submitting Service Requests for Approval and Withdrawing them from Approval can be accessed in the “Take an Action Menu” for the ticket. Notification and Reminders related to Approval process get sent to Approvers / Reviewers and other participants as per workflow configured. Approvers / Reviewers shall be able to view “My Outstanding Approvals” information and interact to record their decisions. Setting the parameter value to “No” disables the approval based routing functionality hides all the above Approval related functions and features.
Default Value	No
Valid Value	Yes/No
Impact Area	Service Request Approval Routing
Appears on Interface	Agent and Admin

SRQ_WORKLOG_REQUIRED_FIELDS_LIST

This parameter manages the fields in the worklog section which are to be marked as Required Fields.

Title	Description
Parameter Name	SRQ_WORKLOG_REQUIRED_FIELDS_LIST
Parameter Description	Set the worklog field where you would like inputs to be mandatory when adding a worklog for Service Requests. The fields specified as mandatory shall require user to provide a value. If the value is not available, a message asking the user to provide the value before saving the Ticket record is displayed.
Default Value	All boxes unchecked
Valid Value	Checkboxes
Impact Area	Service Request Worklog fields
Appears on Interface	Agent

SRQ_INITIAL_SOURCE_FOR_EMAIL_CONVERSIONS

This parameter manages the Initial Source for tickets created via email conversions.

Title	Description
Parameter Name	SRQ_INITIAL_SOURCE_FOR_EMAIL_CONVERSIONS
Parameter Description	This parameter sets the initial Source (origin) for a new Service Request created via conversion of incoming emails into Service Request. The system default is Email. You can use Advanced Search for tickets, where you can search using Source. Populating a specific value into tickets created via conversion of email enables easy search for these tickets.
Default Value	Email
Valid Value	Text from dropdown
Impact Area	Service Request Source Field
Appears on Interface	Agent

Self-Service

The below Slice Configuration Parameters control features and functionality for Self-Service Users (SSU). These parameters are grouped under the Parameter Category “Self-Service” in the Manage Slice Configuration form.

ALLOW_CLOSED_TICKET_MODIFICATIONS_FOR_SSU

This parameter enables SSU to modify closed tickets.

Title	Description
Parameter Name	ALLOW_CLOSED_TICKET_MODIFICATION_FOR_SSU
Parameter Description	When the parameter value is set to “Yes”, a Self Service User (SSU) can modify Closed tickets and also add worklog to it if required. If the value is “No”, the SSU will not be able to modify tickets which are in Closed Status.
Default Value	No

Valid Value	Yes/No
Impact Area	Closed Tickets- Worklog editing by SSU
Appears on Interface	SSU

DAYS_TO_SHOW_CLOSED_FOR_SSU_ON_TICKET_LIST

This parameter controls display of closed tickets on SSU interface.

Title	Description
Parameter Name	DAYS_TO_SHOW_CLOSED_FOR_SSU_ON_TICKET_LIST
Parameter Description	This parameter sets the number of days for which a closed ticket will be displayed on the SSU Interface Ticket list. If the parameter value is set to 1, it means Closed tickets will show for one day after the closure. If set to "0" (zero), Closed tickets shall not be included in the Ticket list.
Default Value	1
Valid Value	0 or Positive Integer
Impact Area	Closed Tickets SSU Home and Ticket List
Appears on Interface	SSU

SSU_VIEW_MY_REQUEST_ONLY

This parameter controls SSU ability to view tickets logged by others in their organization.

Title	Description
Parameter Name	SSU_VIEW_MY_REQUEST_ONLY
Parameter Description	If the parameter value is set to "Yes", the SSU is allowed to view only those requests that specifically belong to the logged in SSU in the Home Page ticket list. If parameter value is set to "No", the ticket list on SSU Home Page will include requests of other users in the SSU organization.
Default Value	No

Valid Value	Yes/No
Impact Area	Inclusion on Organization tickets in SSU Home Page, Ticket List, Search Requests and Global Search
Appears on Interface	SSU

Note:

SSUs who are members of only Self Service Group as their primary group can View Organization Tickets only if this slice parameter is set to NO, and the View Organization Tickets flag for Self Service Users Group to permit View My Organization Tickets is enabled.

If both slice parameter and SSU group flag permit viewing the Organization Tickets, radio buttons are displayed for Request List, SSU Search Request Criteria and SSU Global Search page to enable SSU to include / exclude Organization Tickets from the search results.

SSU who are also member of any additional group (while their primary group remains Self-Service) that permits viewing Organization Tickets, have the radio button option to include Organization Tickets in Request List, SSU Search Request Criteria and SSU Global search. This is so even when Self Service (their primary group's flag) does not permit viewing Organization tickets.

SSU_HIDE_REQUEST_FIELDS_LIST

This parameter controls the display of Priority, Urgency and Type fields on the SSU ticket form.

Title	Description
Parameter Name	SSU_HIDE_REQUEST_FIELDS_LIST
Parameter Description	Select the fields to be displayed or hidden on SSU ticket form. Manage display of three fields - Priority, Urgency and Type on SSU Ticket form. Click on the checkbox of the field name to hide display of the field. When no check box is selected; all three fields will be displayed.
Default Value	All Boxes Unchecked
Valid Value	Checkboxes
Impact Area	SSU's Request - Priority, Urgency and Type fields display

Appears on Interface	SSU

SSU_SHOW_RELATED_CONFIGURATION_ITEMS_SECTION

This parameter controls SSU ability to view and relate Configuration Items to a ticket.

Title	Description
Parameter Name	SSU_SHOW_RELATED_CONFIGURATION_ITEMS_SECTION
Parameter Description	When the parameter value is set to “Yes” it displays the Related Configuration Items section when SSU accesses a Request form to create a new Request. This section allows SSU to search for Configuration Items and select the ones he/she wants to relate to the Request. If the parameter value is set to “No”, the Related Configuration items section is not displayed and SSU cannot relate CIs to Request or view CIs related to the Request by Agents.
Default Value	Yes
Valid Value	Yes/No
Impact Area	SSU Submit Request form
Appears on Interface	SSU

SSU_ATTACHMENT_COMPLIANCE_MESSAGE

This parameter controls the Attachment Compliance message displayed.

Title	Description
Parameter Name	SSU_ATTACHMENT_COMPLIANCE_MESSAGE
Parameter Description	This parameter allows Administrator to compose an alternative Message text to display in the Attachment Section for SSU Request form. If the system default message is not modified, the given default Message gets displayed.
Default Value	Please avoid attaching or uploading files which contain non-

	public personal information.
Valid Value	Text
Impact Area	SSU Request form Attachment section
Appears on Interface	SSU

SHOW_SOLUTIONS_DETAILS_SECTION

This parameter controls the ability for SSU to view Solution Details on resolved tickets.

Title	Description
Parameter Name	SSU_SOLUTIONS_DETAILS_SECTION
Parameter Description	If parameter value is set to “Yes” the Solutions Details section on SSU’s Requests is displayed on tickets with Resolved or Closed status. If the Request is in any other status, the Solution Details section does not get displayed. When the parameter value is set to “No” the Solution section on SSU Requests is hidden irrespective of status of the Request.
Default Value	Yes
Valid Value	Yes/No
Impact Area	SSU Solutions section
Appears on Interface	SSU

SSU_SHOW_COMMUNICATION_WORKLOGS

This parameter controls the display of communication worklogs on SSU tickets.

Title	Description
Parameter Name	SSU_SHOW_COMMUNICATION_WORKLOGS
Parameter Description	This parameter sets restrictions to the communication that is included in SSU Request’s worklog. If the parameter value is set as “None”, no Communication Logs are shown on the ticket.

	When “Only Incoming” is selected, only Communications marked as Incoming are visible to the SSU - i.e. only communications sent by SSU is visible. When both “Incoming and Outgoing” options are selected, all communications are displayed.
Default Value	None
Valid Value	None, Incoming, Incoming and Outgoing
Impact Area	SSU Request – Communication entries in Worklogs
Appears on Interface	SSU

SSU_SEARCH_SOLUTION_MAX_ROWS_DISPLAYED

This parameter manages the number of rows displayed in search solution result list.

Title	Description
Parameter Name	SSU_SEARCH_SOLUTION_MAX_ROWS_DISPLAYED
Parameter Description	Use this parameter to set the maximum number of records that are to be displayed per page of the Results of a solution search from SSU interface. System default value is 50 Records per page.
Default Value	50
Valid Value	Number
Impact Area	SSU Knowledge Management – Search Solution
Appears on Interface	SSU

SSU_MANDATORY_REQUEST_FIELD_LIST

This parameter enables marking fields on SSU ticket as Mandatory Fields.

Title	Description
Parameter Name	SSU_MANDATORY_REQUEST_FIELD_LIST
Parameter	This parameter specifies the fields on SSU Requests that are to

Description	be validated as “Required” fields on submit action. You can choose multiple fields from the options available to be marked as Required fields.
Default Value	Name, Details
Valid Value	Checkbox Options
Impact Area	SSU Request creation and submit
Appears on Interface	SSU

System

The Slice Configuration Parameters listed manage features generic to the System; applicable to a range of users. These parameters are grouped under the Parameter Category “System” in the Manage Slice Configuration form.

SUPPORT_NOTE

This parameter controls the “Support Note” displayed in the Support Information Page under Home.

Title	Description
Parameter Name	SUPPORT_NOTE
Parameter Description	Create a Support Note that will be displayed on the Support Information page under Home section.
Default Value	We offer full technical support to all the currently registered customers and users. If you are having technical difficulties, please feel free to call or email.
Valid Value	Text
Impact Area	Support Information page
Appears on Interface	Agent and Admin

SUPPORT_URL

This parameter controls the display of the “Support URL” in the Support Information page.

Title	Description
Parameter Name	SUPPORT_URL
Parameter Description	Update the Support URL that gets displayed on the Support Information page under Home section.
Default Value	www.nimsoft.com
Valid Value	Text
Impact Area	Support Information page
Appears on Interface	Agent and Admin

SUPPORT_PHONE

This parameter controls the display of “Phone Number for Support” in the Support Information Page

Title	Description
Parameter Name	SUPPORT_PHONE
Parameter	Update an appropriate Phone Number that will get displayed on

Description	Support Information page under Home section.
Default Value	0265 - 2311584
Valid Value	Text
Impact Area	Support Information page
Appears on Interface	Agent and Admin

MAX_AUTHORIZATION_TOKEN_LENGTH

This parameter is currently inoperative. This parameter set the maximum length for Authorization Tokens.

Title	Description
Parameter Name	MAX_AUTHORIZATION_TOKEN_LENGTH
Parameter Description	Sets the maximum allowed authorization token length. Authorization tokens are generated by background process for a contact under specific conditions. This only controls the length of the token. Maximum length is 50. Presently this parameter is not effective and is ignored. Even when the value is 15, it generates authorization token of length 50.
Default Value	15
Valid Value	Number
Impact Area	Currently Not Operative
Appears on Interface	Not visible on GUI

DEFAULT_REPLYTO_EMAIL_PROFILE_NAME

This parameter controls the name displayed for response to Support.

Title	Description
Parameter Name	DEFAULT_REPLYTO_EMAIL_PROFILE_NAME
Parameter Description	The Profile Name provided in this parameter shall be used as a Default reply-to Email address that will be displayed on Emails sent to Service Desk.

	This Default is used even when no delegate Texts are provided in the Slice Configuration parameters EMAIL_DELEGATE_TEXT_FOR_SELF_SERVICE_USERS or EMAIL_DELEGATE_TEXT_FOR_AGENTS in slice parameter category “Service Desk”.
Default Value	Service Desk
Valid Value	Text
Impact Area	Emails
Appears on Interface	Agent and SSU

DEFAULT_LOGIN_ID_TO_EMAIL_ADDRESS

This parameter controls the use of contact email id as default login name.

Title	Description
Parameter Name	DEFAULT_LOGIN_ID_TO_EMAIL_ADDRESS
Parameter Description	When the parameter value is set to “Yes”, the contact person’s Email address shall be used as the system user ID. Setting the value to “No” requires that each contact be assigned a specific System User ID in Manage Contacts (Contact Profile).
Default Value	No
Valid Value	Yes/No
Impact Area	Contact Management
Appears on Interface	Administrator

LOCALE_SPECIFIC_FIRST_DAY_OF_THE_WEEK

This parameter is currently inoperative. It controls the calendar display of locale specific first day of the week.

Title	Description
Parameter Name	LOCALE_SPECIFIC_FIRST_DAY_OF_THE_WEEK

Parameter Description	Currently this parameter is inoperative. In future when it is made operational, the Calendar display will reflect the first day of the week according to the selected country.
Default Value	No
Valid Value	Yes/No
Impact Area	Currently Not applicable
Appears on Interface	Currently Not Applicable

ENABLE_PERSISTENT_SESSION_STATE

This parameter controls system's response when a user who is currently logged into Nimsoft Service Desk attempts to log in again and start a new session.

Title	Description
Parameter Name	ENABLE_PERSISTENT_SESSION_STATE
Parameter Description	When the parameter value is set to "No", the existing (previous) session is not automatically recognized and the Login page will be displayed. If user logs in with same ID and password (as the current logged in session), a message about a current active session in progress will be displayed and the user will be asked to choose to continue after forcefully ending current session; or abort the second login. Finally, only one session will be active and in progress. If the parameter value is set to "Yes", the existing (previous) session will be recognized and Home page will be displayed so that user does not have to login again. However, the older session will be ended. Finally, only one session will be in progress.
Default Value	No
Valid Value	Yes/No
Impact Area	Login for all users
Appears on Interface	All Users

PRIVATE_LABEL_LOGO_IMAGE

This parameter controls display of user organization logo in place of default Nimsoft Service Desk logo.

Title	Description
Parameter Name	PRIVATE_LABEL_LOGO_IMAGE
Parameter Description	This parameter provides path to the Logo Image file that will be used as logo on Home page when the logged in User's Primary Organization and the Organization with ID#1 do not have a specified logo. In the absence of logos for logged in User's Primary Organization and Organization with ID #1, the default Nimsoft Service Desk logo shall be displayed if path is not provided in this parameter for an Image.
Default Value	web/common/img/logos/logo_Nimsoft Service Desk.gif
Valid Value	Text
Impact Area	Logo displayed on Home Page
Appears on Interface	All Users

SINGLE_SIGNON_CONTEXT_URL

This parameter is related to Single Sign on.

Title	Description
Parameter Name	SINGLE_SIGN_ON_CONTEXT_URL
Parameter Description	The URL provided here will be the one that will replace Direct URL of Nimsoft Service Desk. It will replace Direct URL in all communication templates wherever Direct URL is mentioned. It will still be possible for user to type in Direct URL in the browser and work as if Single Sign On is not used. In that case, the communication templates shall pick up Direct URL and not Single Sign On related URL.
Default Value	Blank

Valid Value	Text (Valid URL)
Impact Area	URL displayed on communication templates
Appears on Interface	All Users

ACTIVE_DIRECTORY_USER_SYNC_NOTIFICATION_RECIPIENTS

This parameter is related to Active Directory Synchronization process.

Title	Description
Parameter Name	ACTIVE_DIRECTORY_USER_SYNC_NOTIFICATION_RECIPIENTS
Parameter Description	Active Directory synchronization process with respect to Contacts in Nimsoft Service Desk is independently executed. There are notifications that AD sync process generates. The contacts / Email addresses (semi colon separated) listed here shall receive those notifications.
Default Value	Blank
Valid Value	Text
Impact Area	Contact Management
Appears on Interface	Not visible on GUI

ACTIVE_DIRECTORY_USER_SYNC_DEPROVISION_USERS_NOT_IN_SOURCE

This parameter enables updating Nimsoft Service Desk contact details to user Active Directory.

Title	Description
Parameter Name	ACTIVE_DIRECTORY_DEPROVISION_USERS_NOT_IN_SOURCE
Parameter Description	Default value set to “yes” allows making inactive those Nimsoft Service Desk self-service and non-administrative users that no longer exist in the Active Directory (AD) user source when AD synchronization with Nimsoft Service Desk process is executed. Note that Administrators are excluded.

Default Value	Yes
Valid Value	Yes/No
Impact Area	Contact Management
Appears on Interface	Not visible on GUI

ACTIVE_DIRECTORY_USER_SYNC_DEPROVISION_USERS_THRESHOLD

This parameter controls number of contacts that can be made inactive per AD Sync Process.

Title	Description
Parameter Name	ACTIVE_DIRECTORY_USERS_SYNC_DEPROVISION_USERS_THRESHOLD
Parameter Description	Sets the upper limit for number of Nimsoft Service Desk users that can be made Inactive (deprovisioned) during each execution of Active Directory Synchronization process. If more than these numbers of contacts are deprovisioned, the execution will stop and the process will be rolled back. Incase of Default value (10 contacts) if 11th contact needs to be deprovisioned, the process will stop and restore all 10 contacts to original active state.
Default Value	10
Valid Value	Number
Impact Area	Contact Management
Appears on Interface	Not visible on GUI

ACTIVE_DIRECTORY_USER_SYNC_DEPROVISION_ADMINISTRATORS_NOT_IN_SOURCE

This parameter controls ability to deprovision contacts in Administrator Group during AD Sync.

Title	Description

Parameter Name	ACTIVE_DIRECTORY_USERS_SYNC_DEPROVISION_USERS_THRESHOLD
Parameter Description	Default value set to “No”, does not permit deprovisioning of an administrator user in Nimsoft Service Desk if the same no longer exists in Active Directory (source) being synchronized with Nimsoft Service Desk contacts. If set to “Yes” the active Nimsoft Service Desk administrator contact, not found in Active Directory, shall be made inactive.
Default Value	No
Valid Value	Yes/No
Impact Area	Contact Management
Appears on Interface	Not visible on GUI

DEFAULT_TIMEZONE

This parameter sets the default time zone for the slice.

Title	Description
Parameter Name	DEFAULT_TIMEZONE
Parameter Description	Sets the default or local time zone that applies to this particular slice. Outgoing Emails from Nimsoft Service Desk, when viewed by the recipient need a time stamp of creation. The default time zone clock is used for that purpose.
Default Value	(GMT – 5:00) America/New York/
Valid Value	Select from Dropdown
Impact Area	Time Stamp on all emails from the application
Appears on Interface	Email Communications

MAX_ACTIVE_SCHEDULED_TASKS

This parameter controls the maximum number of Schedules that can be active.

Title	Description

Parameter Name	MAX_ACTIVE_SCHEDULE_TASKS
Parameter Description	Set the maximum number of scheduled tasks (active and queued) that will be allowed to be run automatically by the server.
Default Value	50
Valid Value	Number
Impact Area	Schedule Tasks (Manage Schedules)
Appears on Interface	Agent and Administrator

SYSTEM_DEFAULT_LOCALE

This parameter controls the default locale for all contacts in a slice, where an explicit locale preference has not been set by the contact.

Title	Description
Parameter Name	SYSTEM_DEFAULT_LOCALE
Parameter Description	Set the default locale to be used when a contact record is created or updated through Ad Sync, Bulk Upload, or manual configuration; where an explicit locale preference is not set or defined. The System default locale will also be used in Outgoing email communications to set the date format as per the slice default format.
Default Value	English (United States)
Valid Value	Text from dropdown
Impact Area	Date Formats on Communication and Contact Records
Appears on Interface	All Users

ENABLE_SHARING_OF_LANGUAGE_TRANSLATIONS

This parameter enables sharing of translated content created in a tenant slice with the management slice.

Title	Description
Parameter Name	ENABLE_SHARING_OF_LANGUAGE_TRANSLATIONS
Parameter Description	Setting the parameter as Yes enables sharing of collection of translated text strings specific to a locale and language, created in a tenant slice, with the management slice. This allows the management slice to access translated text strings that have been created within your slice.
Default Value	No
Valid Value	Yes/No
Impact Area	Manage Language Catalog, Bulk Upload of Language Element, Language translation of the labels and data.
Appears on Interface	Not visible on UI

ENABLE_ORGANIZATION_BASED_ACCESS_CONTROL

This parameter allows you to enable or disable Organization Based Security to control access to tickets and Configuration Items based on related Organization.

Title	Description
Parameter Name	ENABLE_ORGANIZATION_BASED_ACCESS_CONTROL
Parameter Description	If this Parameter value is set to Yes, Organization based access permissions to Tickets and Configuration Items is enabled. Logged in users (except Administrators) will be able to access only those Tickets and Configuration Items that belong to an Organization that they are directly or indirectly related to.
Default Value	No
Valid Value	Yes/No
Impact Area	All Ticket Types, Configuration Items. Searches and Reports related to Tickets and Configuration Items.
Appears on Interface	Not visible on the UI

Service Level Management

The below Slice Configuration Parameters control features related to Service Level Management. They are classified under Parameter Category “Service Level Management” in the Manage Slice Configuration form.

SLA_THRESHOLD_VIOLATION_TOLERANCE

This parameter manages the level at which Approaching Violation message is displayed.

Title	Description
Parameter Name	SLA_THRESHOLD_VIOLATION_TOLERANCE
Parameter Description	This parameter sets the criteria to change the SLA Target compliance status from “In Progress” to “Approaching Violation”, for a violation threshold applied to a Ticket. The system default Value is that when the measured value reaches 80% of the elapsed time from a violation target time limit, it changes the SLA compliance status to “Approaching Violation”. For Example: If Threshold value = 10 minutes the Status changes to “Approaching Violation” upon crossing 8 minutes.
Default Value	80
Valid Value	Number
Impact Area	SLA Compliance Information displayed on SLA Compliance Tab for a Ticket.
Appears on Interface	Agent and Administrator

SLA_BUSINESS_SERVICES_IDENTIFIER_CLASSES

This parameter manages the CCTI that will be treated as Business Services.

Title	Description
Parameter Name	SLA_BUSINESS_SERVICES_IDENTIFIER_CLASSES
Parameter Description	This parameter sets the Categorization (CCTI) classes to be treated as Business “Services” when applied to Configuration Items. A Configuration Item belonging to any of these classes can be associated with a Ticket as “Affected Service”.

	An SLA target can be made applicable to specific “Services” and SLA thresholds can be based on Service Metric defined in relation to Availability Hours (schedules) of affected “Service” linked to a Ticket.
Default Value	Blank
Valid Value	Text
Impact Area	Configuration Items and interacts with Service Level management based on Service availability hours
Appears on Interface	Agent and Administrator

SLA_ENABLE_SUPPRESSION_ON_PENDING_ACTIONS

This parameter controls the automatic execution of alerts and escalations based on SLA target thresholds.

Title	Description
Parameter Name	SLA_ENABLE_SUPPRESSION_ON_PENDING_ACTIONS
Parameter Description	If the parameter value is set to “Yes”, the SLA Monitor applies SLA targets to matching tickets, monitors compliance, determines Compliance status, displays information on SLA tabs for the tickets but it does not execute any of the proactive warnings Notification and escalation actions associated with the SLA target Thresholds. The Activity Tab information for the ticket also does not create activity records because no communication / escalation actions are executed. The parameter value must be set to “No” to execute the automatic warning / alert communications and assignment actions based on escalation when thresholds are crossed.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Automatic execution of alerts and escalation actions based on SLA target thresholds
Appears on Interface	Agent and Administrator

SLA_PROCESS_HIGHEST_ACTIONABLE_THRESHOLD_RULES

This parameter manages SLA target based automatic notification and escalation action.

Title	Description
Parameter Name	SLA_PROCESS_HIGHEST_ACTIONABLE_THRESHOLD_RULES
Parameter Description	Default value set to “Yes” permits processing of only the highest (based on Sort Order value) actionable threshold rule and skips thresholds with lower Sort Order values. When set to “No”, all actions based on thresholds already crossed shall be executed. This applies during SLA compliance monitoring process, when a new SLA Target becomes applicable to a Ticket and elapsed time has already crossed some of Threshold values of the new Target. For example, a Ticket is updated such that a new Target becomes applicable. At the time of the SLA monitoring review, two Thresholds with Sort Orders 1 and 2 have been crossed. In that case only actions for Threshold with sort order 2 shall be executed.
Default Value	Yes
Valid Value	Yes/No
Impact Area	SLA Target based automatic Notification and Escalation actions.
Appears on Interface	Agent and Administrator

Task Management

The below Slice Configuration Parameters control features related to Task Management. They are classified under Parameter Category “Task” in the Manage Slice Configuration form.

TSK_INITIAL_STATUS

This parameter manages the default Status value for new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_STATUS
Parameter Description	This parameter sets the initial status for a new Task Ticket. System default Value is New. You can change this to an alternate value. When a new Task Ticket is saved for the first time, the Value for the Status field is automatically set to default value set by the Administrator.
Default Value	New
Valid Value	Dropdown Options
Impact Area	Task Ticket- Status field
Appears on Interface	Agent

TSK_INITIAL_REASON_CODE

This parameter controls the default Reason Code value of new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_REASON_CODE
Parameter Description	This parameter sets the initial Reason Code for a new Task Ticket. The system default Value is None. You can set an alternate value as applicable. When a new Task Ticket is saved for the first time, the Value for the Reason Code field is automatically set to this default value set by the Administrator.

Default Value	None
Valid Value	Text
Impact Area	Task Ticket- Reason Code field
Appears on Interface	Agent

TSK_INITIAL_PHASE

This parameter controls the Phase value for new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_PHASE
Parameter Description	This parameter sets the Initial phase for a new Task Ticket. The system default is Task Ticket Recording. You can choose an alternate appropriate value. When a new Task Ticket is saved for the first time, the Value for the Phase field is automatically set to this default value set by the Administrator.
Default Value	Task Ticket Recording
Valid Value	Text
Impact Area	Task Ticket- Phase field
Appears on Interface	Agent

TSK_DISABLE_USER_EDITING_TICKET_STATUS

This parameter controls the status at which Task Tickets cannot be edited.

Title	Description
Parameter Name	TSK_DISABLE_USER_EDITING_TICKET_STATUS
Parameter	This parameter sets the Status values to restrict Task Ticket

Description	editing. System default Values are Resolved, Closed. You can specify other statuses. Task Tickets in any specified status, cannot be edited by any user and can be accessed in Read Only mode.
Default Value	Resolved, Closed
Valid Value	Text
Impact Area	Task Ticket- Updates
Appears on Interface	Agent

LOCK_TASK_NAME_FOR_TASKS_CREATED_USING_TEMPLATE

This parameter enables locking of task tickets Task Name field.

Title	Description
Parameter Name	LOCK_TASK_NAME_FOR_TASKS_CREATED_USING_TEMPLATE
Parameter Description	When this parameter value is set to “Yes”, the Task Name field is locked for editing for Task tickets created using Task Templates or Request Catalog of Self Service User. If the value is set to “No” it permits editing of Task Name field for Task Tickets created using Task Templates.
Default Value	No
Valid Value	Yes/No
Impact Area	Task Ticket- Updates
Appears on Interface	Agent

TSK_REQUESTER_REPLY_REASON_CODE

This parameter controls the Reason Code set when the requester updates a Task Ticket.

Title	Description
Parameter Name	TSK_REQUESTER_REPLY_REASON_CODE

Parameter Description	This parameter defines the Reason Code to be set on the Task Ticket when an email response is received from ticket's Requester/ Contact Person for the Task. Default is No Value. It enables the Administrator to provide a text (for example, "Responded by User") to be automatically populated in the Reason Code field of the Task Ticket to indicate Email interaction with Requester / Contact Person for the Task.
Default Value	Blank
Valid Value	Text
Impact Area	Task Ticket- Reason Code field
Appears on Interface	Agent

TSK_REQUESTER_REPLY_STATUS

This parameter manages the Status value displayed with the requester updates a Task Ticket.

Title	Description
Parameter Name	TSK_REQUESTER_REPLY_STATUS
Parameter Description	This parameter defines the Status value to be set on the Task Ticket when an email response is received from ticket's Requester/ Contact Person for Task or it is manually updated by an SSU. Default is Blank. Valid Values are Ticket Status values. This enables the Administrator to specify a status (for example, "Queued") to automatically update the Status of the Task Ticket, based on Email interaction with Requester / Contact Person for Task or manual update by Self Service User.
Default Value	Blank
Valid Value	Dropdown Options
Impact Area	Task Ticket- Status field
Appears on Interface	Agent

TSK_ENABLE_CUSTOM_FIELDS

This parameter manages the use of Custom Fields on Task Tickets.

Title	Description
Parameter Name	TSK_ENABLE_CUSTOM_FIELDS
Parameter Description	Setting to parameter value to “Yes” (Default), enables the display of Custom Fields in the Additional Information tab for the Task Ticket. Custom fields allow tracking information in addition to the standard fields for Task Tickets. If the value is set to “No” the Additional Information Tan on the Task Ticket is hidden and custom field related information do not get captured.
Default Value	Yes
Valid Value	Yes/No
Impact Area	Task Ticket- Additional Information Tab
Appears on Interface	Agent

TSK_INITIAL_PRIORITY

This parameter manages the default value for Priority of new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_PRIORITY
Parameter Description	Set the initial Priority for a new Task Ticket. System default is Medium (Code 3). You can modify it to an alternate acceptable value. The default initial value for Priority represents the most common value users may assign and users can change it if necessary for a specific ticket. Providing a default initial value also ensures proper functioning of processes which cannot accept a “Blank” Priority field.
Default Value	Medium
Valid Value	Dropdown Options

Impact Area	Task Ticket- Priority Field
Appears on Interface	Agent

TSK_INITIAL_SOURCE

This parameter manages the default value for Source of new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_SOURCE
Parameter Description	Set the initial Source for a new Task Ticket. The System default is Web (Code 4). You can modify it to an alternate acceptable value. The default initial value for Source represents the most common value users may assign and users can change it if necessary for a specific ticket. Providing a default initial value also ensures proper functioning of processes which cannot accept a "Blank" Source field.
Default Value	Web
Valid Value	Dropdown Options
Impact Area	Task Ticket- Source Field
Appears on Interface	Agent

TSK_INITIAL_URGENCY

This parameter manages the default value for Urgency for new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_URGENCY
Parameter Description	Set the initial Urgency for a new Task Ticket. System default is Medium (Code 2). You can modify it to an alternate acceptable value.

	The default initial value for Urgency represents the most common value users may assign and users can change it if necessary for a specific ticket. Providing a default initial value also ensures proper functioning of processes which cannot accept a “Blank” Urgency field.
Default Value	Medium
Valid Value	Dropdown Options
Impact Area	Task Ticket- Urgency Field
Appears on Interface	Agent

TSK_INITIAL_IMPACT

This parameter manages the default value for Impact for new Task Tickets.

Title	Description
Parameter Name	TSK_INITIAL_IMPACT
Parameter Description	Set the initial Impact for a new Task Ticket. System default is Medium (Code 2). You can modify it to an alternate acceptable value. The default initial value for Impact represents the most common value users may assign and users can change it if necessary for a specific ticket. Providing a default initial value also ensures proper functioning of processes which cannot accept a “Blank” Impact field.
Default Value	Medium
Valid Value	Dropdown Options
Impact Area	Task Ticket-Impact Field
Appears on Interface	Agent

TSK_ENABLE_APPROVAL_ROUTING

This parameter is currently inoperative. It enables approval routing for Task Tickets.

Title	Description
Parameter Name	TSK_ENABLE_APPROVAL_ROUTING
Parameter Description	If the parameter value is set to “Yes” it enables multi-tiered approval routing workflow processes for Task Ticket. When enabled, the Task Ticket shall display the Approval Tab with the relevant details such as Approval Phase, Names of Approvers/ Reviewers, status of Approval Decisions by them, etc. In addition, Workflow actions configured by Administrator for Submitting Task Ticket for Approval and Withdrawing them from Approval can be accessed in Take an Action Menu for the ticket. Notification and Reminders related to Approval process shall be sent to Approvers / Reviewers and other participants as per workflow configured. Approvers / Reviewers shall be able to view “My Outstanding Approvals” information and interact to record their decisions. When parameter value is set to “No” approval routing for Task Tickets is disabled and all the above Approval related functions and features are hidden.
Default Value	No
Valid Value	Yes/No
Impact Area	Task Ticket-Approval Routing
Appears on Interface	Currently Not Applicable

TSK_WORKLOG_REQUIRED_FIELDS_LIST

This parameter manages the fields in the worklog section which are to be marked as Required Fields.

Title	Description
Parameter Name	TSK_WORKLOG_REQUIRED_FIELDS_LIST
Parameter Description	Set the worklog field where you would like inputs to be mandatory when adding a worklog for Task Tickets. The fields specified as mandatory shall require user to provide a value. If the value is not available, a message asking the user to provide the value before saving the Ticket record is displayed.

Default Value	All Boxes unchecked
Valid Value	Checkboxes
Impact Area	Task Ticket-Worklog fields
Appears on Interface	Agent

DEFAULT_REQUESTER_FOR_TASK_TICKETS

This parameter controls the default requester details on Task Tickets.

Title	Description
Parameter Name	DEFAULT_REQUESTER_FOR_TASK_TICKETS
Parameter Description	Set the default Requester for Task Tickets using this parameter. The system default is Logged in Individual. You can choose from the available valid options. The Requester and Requested For of the task ticket will be set as per the above configuration in all the task creation scenarios. If the Requester cannot be resolved to a valid contact for whatever reason, the Requester will be set to blank.
Default Value	Logged in Individual
Valid Value	Logged in Individual / Parent Ticket's Requester / Parent Ticket's Owner
Impact Area	Task Ticket- Requester tab
Appears on Interface	Agent

ENABLE_AUTO_ROUTING_OF_TASK_TEMPLATES

This parameter enables applying auto routes to Task Templates.

Title	Description
Parameter Name	ENABLE_AUTO_ROUTING_OF_TASK_TEMPLATES
Parameter	If the value is set to "No", the system will continue to behave in

Description	the current manner and no Auto Routes shall be applied to the tasks created using the templates from Task Information Tab or Auto Create Task workflow action. If parameter value is set to “Yes”, it will disable the “Auto Assign Action” functionality. The “Auto Assign Action” and “Assign on Create” fields on the Task Template screen will be disabled. Also, the “Assign All” field on the tickets will be disabled. In this case the system will automatically assign the tasks based on the “Auto Routes” defined, with “Override Auto Routing” flag for Template set to “No”. The user should be able to reassign the tasks after creation in the usual manner. The administrator can also use the “Override Auto Routing” flag to prevent the specific templates from getting auto routed.
Default Value	No
Valid Value	Yes/No
Impact Area	Task Tickets (Using Template) leading to Auto Route
Appears on Interface	Agent and Administrator

Frequently Asked Questions

Below are answers to some questions you may have related to Configuration Parameters

What do the Configuration Parameters control?

Configuration Parameters allow you to modify how the application works for you to some extent compared to its default functionality and allows you to turn on or turn off identified functionality.

Do new configuration parameters get added every time there is a new release?

If there is a new functionality where there is need to maintain backward compatibility, a new slice parameter gets added. This allows maintaining backward compatibility and allows you to choose to adopt or not adopt the new functionality.

Can I modify a parameter at any stage after using the application?

Yes; you can choose to modify a Slice Parameter whenever you deem appropriate. However, you must exercise due caution when turning off a functionality that has been in use as this may cause some mismatches in existing/active transactions and also confuse Service Desk Agents working on the tickets.

Chapter 36 – Administration Utilities

Overview

After setting up all required records in Nimsoft Service Desk and configuring the application to automate and manage your IT Support needs, the Application Administrator is involved in the assisting and supporting users use the application effectively.

Besides responding to user queries, you would be required to undertake activities like manage User Session, Ticket Locks, reset user password, view communication history, or undertake other activities to assist the Agents or Self-Service Users.

This section lists the actions available under the Administration Utilities Section in the Navigation Menu and explains the actions that the Application Administrator will take up as part of the ongoing maintenance of the application.

Links and Actions

The Administration Utilities section provides links to forms that enable the Application Administrator in routine maintenance related tasks and actions. The links in this section are explained below.

Reset User Password

Users of Nimsoft Service Desk (Self-Service Users and Service Desk Agents) can manage their own password from the Change Password link in the Navigation Menu. If required, you can reset the user password to provide either a system generated password or a Custom Generated Password.

The Reset User Password link under Administration Utilities allows you to manage user password reset requests. To reset user password, you can search for the contact name by entering the contact name or login ID in the Search field. A list of matching records gets listed in the table.

Administration Utilities (Reset Users Password)

To find a contact: Please enter First Name, Last Name, Email, Phone and User Id and then click on "Search" button

Search User: [] Search

ID	Full Name	Phone Details	Number	Email	Job Title
53	Beucus, John	Company	1-646-789-8346	jrb@twps.com	CEO
80	Cardoni, Julia	Business	646-739-8524	j.cardoni@bestsm.com	BestSM SDM
54	Lombardino, James	Business	1-646-789-9324	jkl@twps.com	VP Engineering
96	MacLedy, Jack	Business	00 44 161 237 4...	jpm@twps.com	RM- Mancjester UK
86	Rassmussen, Harris	Business	617-362-5768	hir@twos.com	VP HR

Record(s) 1 to 6 of 6

Reset User Password #53 : Beucus, John

Apply Changes Reset Password

Reset Manually System Generated

Reset Password Details

Contact Name: [Beucus, John]

Login ID: [CEXO]

New Password: []

Re-Type New Password: []

Click on the name of the contact whose password is reset, and the login credentials get populated in the appropriate field of the Reset Password form. This form allows you to choose either a System Generate Password for the contact or type in an alternate password manually.

- To assign a system generated password - click on Reset Password action button.
- To manually assign a password- enter the password in the new Password field and click on Change Password.

The password will be changed accordingly and a system generated password changed notification will be sent to the contact on the via email.

Note:

If Email ID is not configured for a contact record, you will not be able to execute the Reset Password Action. A message indicating that the password cannot be reset will be displayed.

Manage Sessions

To access Nimsoft Service Desk; contacts in your instance need to have System User IDs and they have to be assigned an appropriate license. A contact can be assigned Self-Service License, Floater License, or a Fixed License. If you are using web-services, the contact could be given a Web-Services License.

The license controls the number of users who can log in and use the application at the same time. While a contact with a Fixed License uses the license exclusively; Self-Service Users and contacts with Floater License share licenses. While there are a limited number of Self-Service and Floater licenses, the number of users using the license is generally more. This is because not all users remain logged into the application at a time.

Terminating Active Session:

When users log into Nimsoft Service Desk, a Session gets logged. The Session is terminated when the user logs out of the application or the session is otherwise ended.

As Application Administrator, you can view details of all logged in users and, if required, can forcibly terminate one user Session to accommodate another user. You can access the Session details from the Manage Session link under Administration Utilities. Clicking on this link displays the Session Details page, where you can view details of the logged in user.

The table allows you to terminate a user Session. If required, you can terminate an active session and end the user session. However, when the session ends forcibly, the user can lose any unsaved changes or modification he/she has made during the session.

Session Related Configuration Parameters:

A user can log into the application only once at a time. As application administrator, you can manage how Nimsoft Service Desk responds when a user attempts to log into the application again using the same login credentials.

When the ENABLE_PERSISTENT_SESSION_STATE Slice Parameter is set to Yes, the active session is recognized by Nimsoft Service Desk and the Home Page is displayed directly without the user needing to log into the application again. However, here the first session is automatically terminated and a new session is initiated. The user may lose any unsaved changes or transactions.

When the ENABLE_PERSISTENT_SESSION_STATE Slice Parameter is set to No, the active session is not recognized and the Login page is displayed. When the user provides login credentials matching an already active session, a message indicating that there is an active session is displayed. The user can click OK to forcibly terminate the older session and initiate a new session or cancel the request to start a new session.

Manage Ticket Locks

Ticket record all transactions related to a request. The Ticket changes hand during Ticket's Life Cycle and at different stages, different support groups handle the ticket and work on it. At different stages, there are changes and updates to the ticket fields. These can be manual changes done by adding or modifying existing details on the ticket or status changes due to actions taken on the ticket.

Ticket Locks refers to a state when the ticket can be accessed in a Read Only Mode. A user can see the ticket and view all details but the only input allowed is that of adding a Worklog to the ticket to update some information. All other fields are disabled and no action can be taken on the ticket.

Tickets get automatically locked for Self-Service Users; the Ticket is locked once the request is submitted. For Service Desk Agents, when a ticket is being modified by one user; it becomes locked for all other users.

As Application Administrator; you can unlock tickets that have been locked from the Manage Ticket Locks link under Administration Utilities. Clicking on this link will display a Manage Ticket Form. The form displays a Locked Tickets List, which provides details on who has locked a ticket and when. To unlock a ticket, you can Remove the lock from the ticket and make it available for other users.

Unlocking a ticket makes the ticket available for modification to Service Desk Agents who work on the ticket. Self-Service Users will not be able to make any modifications to a ticket even if the ticket is unlocked.

Ticket Lock related Configuration Parameters: Besides the automatic locking of ticket that is being modified, Ticket Locks in other conditions are controlled by Configuration Parameters. These include:

- A ticket submitted for approval
- Specified Status of a ticket.

If the LOCK_TICKET_DURING_APPROVAL is set to Yes, a ticket that is submitted for approval gets locked when in the Approval Process. The lock gets automatically removed after the ticket is approved or rejected.

When managing the initial ticketing functionality, you specify the status at which a ticket should be locked. This setting can be individually modified for each Ticket type. The default type is Resolved and Closed; this means that when a ticket is in Resolved or Closed status, it is locked and cannot be modified. You can modify this parameter to include or exclude available statuses.

Manage Navigation Menu

Nimsoft Service Desk follows a convention of 'What you See is What you Get' to control what users see and do with the application. Self-Service Users and Service Desk Agents can see all those forms and actions that they are permitted to access and use.

For example, consider a user who is logged in as a Service Desk Agent. If the user can see a link for My Dashboards under Home and a list of four Dashboards related to different ticket types, the user will be able to click on the link and view the dashboard.

Some other Service Desk Agent may not be able to see the My Dashboard link at all and would therefore be unable to access any Dashboard.

As application administrator, you have access to all actions and links in the Navigation Menu. Depending on the role a contact plays in IT Services and Support, you can enable or disable access to a particular item in the Navigation Menu.

You can view details of all items in the Navigation Menu for Self-Service Users and Service Desk Agents in Manage Navigation Menu link under Admin Utilities. Clicking on this link displays a list of all items in the Navigation Menu. You can filter the list using available filters.

Administration Utilities (Manage Navigation Menus)

Filter By: Form Name Navigation Menu Group Search

ID	Related To Form	Navigation Menu Group Name	Navigation Menu Name	Sort Order
14	Home	Change Management	Search Change Requests	530
16	Home	Incident Management	Search Incidents	330
17	Home	Request Management	Search Service Requests	230
18	Home	Task Management	Search Task Tickets	610
20	Home	Workflow Tools	Manage Workflow Actions	1910

Record(s) 1 to 20 of 99

Navigation Menu #4 : Manage Roles

Related To Form: Navigation Menu Group Name: Navigation Menu Name: Sort Order:

General Information **Permissions** Manage Permissions

Navigation Menu Code

```
try(getObject("ESD_HCM001_LBL_FORM_TITLE").innerHTML="Application Setup (Manage Roles)");catch(e)
{window.openFrame("ESD_HCM001_FRA_HOME_MAIN","ESD_ADM024_FRM_ROLES_LIST","",no);}
```

When you click on any item in the list, the related details get populated in the form below. The details section displays the Navigation Menu item code. You can manage permissions to an item in the Navigation Menu by enabling or disabling permissions from the Permissions tab.

Manage Toolbars

Service Desk Agents access different ticket forms and also work with Configuration Items records and Knowledge Base Articles. The Toolbar of the Ticket forms, CI form, and KB Article form allow the Service Desk Agents to perform a range of actions on the records. A default set of items are made available on the toolbar of these forms.

Service Desk Agents interacting with the form can perform all actions available to them from the Toolbar. For example, if a Service Desk Agents accesses a Ticket Form and has access to an action called 'Print', the Agent can execute the action of Printing the ticket in an appropriate format.

As Application Administrator, you can enable or disable the ability of Service Desk Agents to access items on the Toolbar and thereby control their ability to take on an action using the option in the Toolbar.

You can manage Toolbar options from the Manage Toolbar link under Administration Utilities. The table lists all available toolbar items. You can filter the list using the available options. When you click on an item in the list, the details get populated in the form below.

Administration Utilities (Manage Toolbars)

Filter By: Form Type Search

ID	Toolbar Name	Toolbar Item	Toolbar Code	Sort Order
98	Save	Save	save();return;	300
58	Add to Knowledgebase	Add to Knowled...	if(hasChanged) { if(confirm("@msg.ESDCOM0015")) { if(isa...	900
84	Manage Global Issue	Unmark as a Glo...	if(!document.getElementsByName("this_ticket_is")[0].checked){...	801
121	Delete	Delete	if(confirm("@msg.ESDADM0041")) {runAjaxAction(getObjec...	500
119	Save	Save	save();return;	200

Record(s) 1 to 20 of 24 << >>

Toolbar #86 : Unrelate from Global Issue Apply Changes Create New Delete

Related To Form: Incident, Problem Toolbar Name: Manage Global Issue Toolbar Item: Unrelate from Global Issue

General Information Permissions Manage Permissions

Toolbar Code:

```
if(!document.getElementsByName("this_ticket_is")[1].checked){alert("@msg.ESDITM0022"); return;} else {runAjaxAction(getObject("form").value,"ESD_handleGlobalIssueAct&actionType=Unrelate&row_id="+row_id);}
```

A default set of permissions are assigned across all groups. You can enable or disable access to different support groups and roles from the Permissions tab of the Manage Toolbar form.

Manage Report Configuration

Nimsoft Service Desk Users can access a range of reports related to Tickets, Configuration Items, Knowledge Management, and Service Feedback. These reports can be accessed from within the respective module of the application. All these reports can also be accessed from within the Trends and Metrics Module of the application.

You can enable or disable access for Service Desk Agents and other Support Groups and Roles to access the available reports.

Modify Reports:

You can access and manage reports from the Manage Report Configuration link under Administration Utilities in the Navigation Menu. Clicking on this link displays a set of Pre-Configured reports that can be accessed from the different ticket and non ticket modules. You can filter the list to view reports related to a specific form type.

To view all details of a chosen report, you can click on a report in the table. The details get populated in the form below.

Administration Utilities (Manage Report Configuration)

Filter By: Form Names

ID	Report Name	Report Description	Sort Order
63	Work Efforts Trend	Displays a trend analysis showing the total time actually spent (in min...	113
64	Work Efforts Trend By Group	Displays a support group wise trend analysis showing the total time a...	114
65	Work Efforts Trend By Individual	Displays a support technician wise trend analysis showing the total ti...	115
66	Open Tickets Aging Report	Displays the number of open tickets in different aging periods groupe...	1
67	Open Tickets Aging Report By Group	Displays the number of open tickets in different aging periods classifi...	2

Record(s) 1 to 20 of 72

Report #61: Tickets Volume and Backlog Trend By Group

Apply Changes Create New Delete

Report Name
Tickets Volume and Backlog Trend By Group

Report Key
esd-itm-ticketVolumeTrendByGroup

Report Description
Displays a support group wise trend analysis showing the number of incoming tickets versus the total resolutions and backlog (unsolved tickets) during the past X days, weeks, or months.

General Information **Permissions** **Manage Permissions**

Related To Form
Home

Category Name
Delivery Trends

You can modify report details like Report Description and add or remove Related to Form Name. You can also change the grouping applied to the report in the Trends and Metrics section and the sort order to control where the report appears in the table.

However, you will not be able to modify the Report Key which determines the nature of the report.

You can enable or disable access to a specific report from the Permissions tab. You can assign or revoke Permissions granted to a contact, support group, or role.

Create Reports:

You can also create new reports using one of the available Report Keys. When you choose a report name from the available list, the Report Key and other relevant details get updated. You can make any required modifications and save the new report.

You can also permanently delete a report. It will be removed from the Manage Report Configuration list. You can manage access to a new report by managing permissions from the Permissions tab.

Search Communication History

Nimsoft Service Desk is capable of sending and receiving communication related to a ticket. The application administrator can configure email notifications to be sent automatically upon a transaction in the application. Service Desk Agents can also manually send communication to intended recipients for different transactions.

The application is also capable of receiving incoming emails and processing them further. Incoming communications either get appended to existing tickets or they are logged as a New Ticket in the application.

As application administrator, you can view details of all incoming and outgoing email notifications from the application. You can access the Communication History by clicking on the Search Communication History link under Administration Utilities. The available search filters will be displayed in the Search Communication History form.

You can enter your search criteria and make modifications to the command as appropriate. For example, if you are looking for a specific notification in the list, you can set the search criteria appropriately and click enter. The search results will be displayed in the Search Results tab. You can see details and status of all communications sent or received.

Service Desk Agents can schedule their communication to be sent at a later date and time. If a communication is scheduled and not dispatched, you can delete the communication, if so required. However, only communication which is Scheduled and not yet Delivered or queued can be dispatched, if needed.

Manage Logon Notice

As part of routine maintenance of the application or other maintenance of the IT services; there could be a planned outage of Nimsoft Service Desk. As application administrator; you can publish a notice about the unavailability of the application during a specified time period. This function is particularly useful for customers having On-Premise installation of Nimsoft Service Desk.

You can set up the notice by clicking on the Manage Logon Notice link under Administration Utilities. Clicking on this link displays the form that allows you to set up the notice.

The actions you can take related to the notice are:

- Create the Notice Header and Notice Content - both fields are editable. You can modify the default text on the form
- Enable or disable the notice
- Choose whether the notice should appear only for Administrators or for All users
- Choose a time duration for which the notice should appear.

Based on the options set; the notice will be displayed on the Home Page after the users have logged into the application.

For customers using the application on SaaS model; when the outage is planned and scheduled by Nimsoft Support, the maintenance or unavailability notice is published by the Super Administrator.

Hence, for SaaS customers, the need to set up the Logon Notice does not exist. As administrator, you can choose to publish a parallel notice. However, at one time; only one notice gets displayed. The following rules apply for the interaction between the Application Administrator and Super Administrator in terms of the Notice.

Sr. No	Notice by Super	Notice by Application	Notice Displayed

	Administrator	Administrator	
1	Notice in force	None	Notice by Super Administrator gets displayed on login page
2	None	Notice in force	Notice by Application Administrator gets displayed on Home Page after login
3	Notice in force	Notice in force	Notice by Super Administrator gets displayed on log in page

The notice gets displayed on the home page for the duration set while configuring the notice. When the combined notice is in force; the notice gets displayed for the longer duration of the display duration set by either the Application Administrator or the Super Administrator.

Predefined Searches

Nimsoft Service Desk provides out-of-the box defined searches for administrative records related to Organization, Site and Location. Similar to the pre-defined search options available for Tickets and Configuration Items, the pre-defined search results are displayed in the Search Results page.

You can export the results into PDF or CSV files and use the output of the search for actions like preparing the Bulk Processing Data sheet for deleting unwanted Organization, Site and Location records.

Manage Language Catalog

End-Users of Nimsoft Services Desk (including Administrators, Agents/Analysts and Self-Service Users) can opt to view and interact with Nimsoft Service Desk in a language other than English. Users can set their preferred locale option and view the application in other supported languages.

All System defined entities like fields labels etc are made available to the end-user as out-of-the-box translations in the supported languages.

In order to facilitate a complete user experience in using the application effectively in the selected language; in addition to the System managed language catalog, you can define translations for fields and attributes that you have configured. This includes elements like Custom fields (Attribute Names and Attribute Values) Workflow Action Option Names, Communication Template Names, etc.

You can undertake the task of compiling your customized language catalog from the Manage Language Catalog form under Administration Utilities. Clicking on this link displays the Language Catalog form.

Key	English Text	Translation Available
Action Option	Action Option	English (United States)
Action Required	Action Required	English (United States)
Action Taken	Action Taken	English (United States)
Action Taken History	Action Taken History	English (United States)
Active	Active	Chinese (China), English (United States), Japanese (Japan), Por ...
Active Directory (AD) User Details ...	Active Directory (AD) User Details ...	English (United States)
Active Projects	Active Projects	English (United States)
ACTIVE_DIRECTORY_USER_SYNC...	ACTIVE_DIRECTORY_USER_SYNC...	English (United States)
ACTIVE_DIRECTORY_USER_SYNC...	ACTIVE_DIRECTORY_USER_SYNC...	English (United States)
ACTIVE_DIRECTORY_USER_SYNC...	ACTIVE_DIRECTORY_USER_SYNC...	English (United States)
ACTIVE_DIRECTORY_USER_SYNC...	ACTIVE_DIRECTORY_USER_SYNC...	English (United States)

In this form you can collate field names, descriptions and Attribute values in your slice and provide translated strings for these items. You can view these elements configured in English and provide the relevant translations in the Manage Language Catalog form.

When you view the form for the first time, the form will be blank with no Language Elements in the list. To collate all custom defined items in your slice, click on the Update Elements Action Button.

All items that can be translated will be displayed in the language elements form. The Translation Available column on the form will display information on which languages the translation has been made available. If a language element or key has not been translated into any language, the message displayed will be English (United States), indicating the same.

You can provide translations for a Key in the Language Elements from by clicking on the Key you want to translate. The item will be displayed in the Translations tab; where you can select the language in which you will make a translation available.



In the Translated Text field, you can type in the translation for the Key in the selected language and click on the Add icon to add the translation.

Note: The Key in English and the translated texts in other languages can be a maximum of 4000 characters. However, for Japanese and Chinese, the field might not support 4000 characters as these languages use double byte characters.

Once the text string is translated; it becomes available in the translated language to a logged in user with the locale preference set as the language in which the text was translated.

So, if you provide a Chinese translation for a Key, and a logged in user has chosen Chinese as the locale, the translated item will be available to the logged in user in Chinese.

Note: You will have to create the original element in English Only. You cannot create an entity or element in a different language, and then provide an English translation for the element. There are other exceptions related to the items you can translate. Please refer to the Internationalization page for further details.

How Do I

Below are some actions you can take related to managing Navigation Menu

Control access to various modules and links in the Navigation Menu

You can control the ability of users to access various modules and links in the Navigation Menu by assigning Permissions to Users, Support Groups, and Roles.

To Control access to various modules and links in the Navigation Menu:

Step 1: Click on the Manage Navigation Menus link under Administration Utilities. The List of Navigation Menus will be displayed.

Step 2: Click on a Navigation Menu item that you wish to modify access to.

The menu details will get displayed in the form below.

Step 3: Click on the Permissions tab of the record.

A list of users who have been granted permission to the link or module will be listed.

Step 4: Click on Manage Permission button to open the Permission Editor lookup.

Step 5: Choose names of contacts, support groups, or roles from the "Select the permissions to be granted" list and click Add.

The chosen names get displayed in the list under "Current Permission".

Step 6: Choose names of contacts, support groups, or roles from the list under "Current Permission" by clicking the checkbox against their names and click Remove to disable permission to the selected contacts.

Step 7: Click Close to close the Permissions Editor.

A list of contacts, support groups and roles to whom Permission has been enabled will be displayed in the form.

Note:

By default Permissions for all actions and records is enabled for Administration Group; enabling all contacts who are part of Administration Group (with Fixed/Floater license) to access the full suite of actions and records. You cannot disable permissions for this Group.

Control items available on the toolbar

You can control the items available on a Ticket Toolbar, Configuration Item Toolbar, and Knowledge Article Toolbar by enabling or disabling permissions to the item.

To control availability of an item in the toolbar:

Step 1: Click on the Manage Toolbar Menu link under Administration Utilities. A list of all Toolbar Items will be listed in the form.

Step 2: Click on the Toolbar Item that you wish to manage access to.

The Toolbar Item details will be displayed in the form below.

Step 3: Click on the Permissions Tab to view details on permissions currently enabled for.

To provide or revoke permissions, click on the Manage Permissions action button. The Permissions lookup will be displayed.

Step 4: Select contacts, users, or roles to whom you wish to enable permissions in the Select Permissions to be Granted section.

You can revoke permission by selecting the user, support group, or roles and clicking on Remove.

By enabling or revoking permission to an item on the toolbar, you can control the actions that Support Technicians or Agents take on a ticket, configuration item or Knowledge article.

Note:

You can also configure a new Toolbar Item. However, the Toolbar Code that you configure has to be logical to render the toolbar item in the menu.

Delete a scheduled communication

Service Desk Agents working on a ticket can schedule communications to be sent out from the ticket at a future date and time. After scheduling the communication, they may decide to cancel the communication.

You can delete a Communication only if the status of the communication is Scheduled. If a notification is in queued or dispatched status, you will not be able to delete it.

You can delete the scheduled communication from the ticket or from the Search Communication History link. To delete the communication from the Search Communication History link:

Step 1: Click on the Search Communication history link to view the Search Communication form. You can search for the communication using any available search criteria.

The search results will be displayed in the Search Results Tab.

Step 2: Click on the Communication that you wish to delete. The communication will open up in a new page.

Step 3: The Delete Option will be visible on the Communication form if the Communication is still in Scheduled status.

You can click on 'Delete' to delete the communication.

Note:

The Service Desk Agent who created the communication can also delete the communication from within the ticket. The scheduled communication will be listed in

the Activity Tab of the ticket. The Agent can view the communication and delete the communication if it is still in Scheduled Status.

However, a Service Desk Agent will not be able to delete communication scheduled by another Service Desk Agent.

Frequently Asked Questions

This section lists questions you may have regarding managing Administrative Utilities such as User Passwords, Sessions, Ticket Locks, Toolbar Menus, Report Configuration, Navigation Menu Items, and Communication Logs.

Can Agents be allowed ability to reset user password?

The reset password link is available as part of the administrative modules. However, if you wish to enable access to this link for users designated as Service Desk Agents, you can do so. You can enable permission for access to the Reset Password action to identified users, support groups, or roles.

How is a contact notified when the password is reset?

A contact is notified via a system generated email about the password being reset.

How is the action by using the Action Button - "Apply Changes" different from the action using "Reset Password" Action button on the Reset Password Form?

You can use the Apply Changes option to manually reset the user password. You can use this option if you wish to manually communicate the changed password to the contact.

The Reset Password action initiates an automatic system generated password which is sent out as an email notification to the contact.

Can contacts reset their own password?

Yes, contacts can change their own password using their own login. The Change Password action on the Self-Service User interface and on the Agent/Admin Interface of the application can be used by the Contact to change their password.

How many sessions can run concurrently?

The number of sessions that can run concurrently depends on the number of licenses that your organization has procured. There can be as many numbers of sessions as the total of Self-Service, Floater, and Fixed licenses that you have bought.

Can I forcibly terminate the session of a logged in user? What is the impact of this?

You can forcibly terminate the session of a logged in User by ending the active user session. However, if there are open records that are being modified when the Session is terminated, the unsaved changes will be lost when the session is terminated.

Can a user have multiple sessions using the same login credentials?

No; a user can log into the application only one at a time or there can be only one Active session with a specified login credentials. If a user who is already logged into the application tries to log in again, the first session will get terminated before the second session is started.

When does a ticket get locked?

When a ticket is opened for viewing or for modification by a logged in user (Service Desk Agent), the tickets get locked automatically.

No modifications can be made to the locked ticket. Only edits possible are adding a worklog.

You can also impose Ticket Lock for tickets submitted for approval by setting Slice Configuration LOCK_TICKET_DURING_APPROVAL as Yes.

Are there any implications of unlocking a locked ticket?

Unlocking a locked ticket makes it available for editing. Ticket locks help in ensuring that a ticket that is being modified by one logged in user does not get modified by another user at the same time.

If more than one user makes changes on a ticket at the same time, there may be conflict in ticket values and this could lead to failure of the planned action to be executed on the ticket.

Can I add new items to the Toolbar?

Yes, you can add new items to the Toolbar. To add a new item, the Toolbar Code has to be correctly configured for the item to be reflected on the selected form.

What is the impact of changing permissions for available items in the Toolbar - will it impact existing records?

Yes; the toolbar item will be available on all existing and new records to which the user has been granted permission. For example, if you have enabled permission to the Ticket Toolbar menu item "Add to Knowledgebase" then this option will become available to the user for all existing and new tickets to which the menu item is related.

What are the records for which I can manage Toolbar Options?

You can manage Toolbar options for all five Ticket Types, Configuration Items, and Knowledge Base Articles.

Can I create new reports specific to my organizational needs?

You can create new reports using an available Report Key. However, you cannot create a new report key for drawing out reports that are unique to your organizational requirements.

What happens when I delete a report?

Deleting a report results in the report being removed permanently from all lists where the report can be accessed from.

You cannot set the status of a report as Inactive and then make it active again.

Will I be able to retrieve a report that I delete and make it active again?

All reports that are configured use a Report Key. If you wish to re-configure a deleted report, you can create a new report with the available Report Key. The Report Key lookup displays a list of all keys that can be used for configuring reports.

Can I add new items to the Navigation Menu?

Yes, you can add new items to the Navigation Menu. To add a new item, the Navigation Menu Code has to be correctly configured for the item to be reflected on the selected form.

Will changes in permissions assigned become visible immediately?

Yes; the Navigation Menu link or section will be available immediately to the logged in user if permission is assigned to the user. Refreshing the screen will display the newly added Link/Section for the logged in user.

If permission is revoked, the availability of the link (and thereby access to the record or form) will be disabled immediately.

Can I enable permission for Self-Service Users for access to an item in the Agent/Admin Interface of the application?

While the application will not stop you from enabling permission for an administrative form for a Self-Service User, the Self-Service User will be able to view and access only those links and forms which are available from the Self-Service User interface. Therefore, enabling permission for the form/link will be meaningless.

Can Agents search for communication history?

Service Desk Agents can view communication history related to a specific ticket in the Activity Tab of the ticket.

The Search Communication History action is made available as part of the Administrative Modules. However, you can allow contacts designated as Service Desk Agents to Search Communication History by enabling permissions to the Navigation Menu item to identified users, support groups, and roles.

What actions can I perform with the records that I see in the communication logs?

You can search for communication logs using the search filters that are available. You can view details of a communication sent; including the status of the communication (whether it was sent or not).

If a Communication is Scheduled (but not queued), you can delete the communication record.

Can I extract details of the Communication logs for reporting or other functions?

Yes, you can extract the Communication Logs into a CSV or PDF file.

The Search Results table allows you to extract the list into a CSV or PDF file.

Chapter 37: Glossary

Seen below is a list of glossary of terms used in the product documentation. They form a part of the explanations or UI labels that have been explained in context of their use in Nimsoft Service Desk. Where the term can be used to explain more than one aspect or functionality, all possible uses have been defined.

The Self-Service User Guide and the Agent User Guide have glossary of terms that are native to their respective sections. You can refer to the Glossary of terms in these, if required.

Action Options

Action Options refers to the options available in the Take An Action option on the ticket toolbar. The Action Options visible in the Take An Action option are controlled by the ticket workflow designed by the Administrator. The Action Options list only those actions that the agent can take on a ticket at a given stage of the ticket life-cycle. This means that the Action Options available will vary depending on the current status of the ticket. The selected Action Option determines the status and reason code of the ticket.

Active

Active refers to the status associated with an entity or record in Nimsoft Service Desk. Active is a status associated with Ticket Status, Configuration Item Status, Solution Status, as well as status of Organization, Site, Location, Support Group, or Contact records.

Active, when used in the context of Ticket Status, means that the Ticket is currently being worked upon. This means that someone has acknowledged and accepted ownership of the ticket but has not completed work on it (or set it to resolved).

Active, when used to refer to Status of other entities like Configuration Item, Workflow Action, Contact etc., implies that that the entity is available and it can be used for transactions like relationship to tickets and other records in Nimsoft Service Desk. Only Active records can be used for any transaction in the application.

Only those records which are active will show up in a search for the respective record. For example, when an SDA wants to associate a user as requester of a ticket, only those users whose status is Active and who belong to an Organization that is Active in Nimsoft Service Desk records, will get displayed in the Name Search Look-up.

Activity Log

Activity Log refers to a record of all actions that have been taken on a ticket logged in Nimsoft Service Desk. Nimsoft Service Desk maintains a record of all Actions like status changes made by the routing engine via any Auto Routes, manual Actions via the Take an Action option, worklogs added to the ticket, and communications sent and received from the ticket.

All this information is classified as Activity Log and is maintained in the Activity tab of the ticket. Users can view the Activity Log to understand the actions that have been taken on the ticket and view communications sent from and received by the ticket. Users can view activity on related tickets if they can also filter the Activity logs to view only Activities of a particular type or logged by a particular user or routing engine.

Active Sessions

An active session indicates that a user is currently logged into the application and the session is live. A list of all active sessions can be viewed from the Manage Sessions link.

Activity Tab

The Activity Tab is a tab that appears on a ticket once it is logged (and assigned a ticket number). This tab contains details of all the activities and actions that have been done on the ticket since it was logged. The activity log can be seen in the Activity tab of the ticket.

Additional Information

The Additional Information tab of the ticket contains customer defined Customs Fields on the ticket forms. For certain standard requests, the Administrator may wish to include Additional Fields over and above the standard ticket fields available by default in the ticket form. The Additional Information tab appears on the ticket form after the ticket is saved/logged.

Affected Services

Configuration Items belonging to a particular class and assigned a particular CCTI by the Administrator, are called Services. If a ticket is logged to report an issue on a specific IT service, Agents can associate the Service with the ticket. The Affected Service field allows agents to associate a service to the ticket.

Anonymous Feedback

Service Feedback Schedule can be configured to solicit feedback from the end users of support. In certain cases, users may be reluctant to submit feedback if they have to disclose their identity. To avoid this, Anonymous Feedback can be sought. You can mark a Service Feedback Schedule as Anonymous and let users submit feedback anonymously.

Application Administrator

Administrators are Contact(s) who are instrumental in setting up Nimsoft Service Desk as per the requirement of the customer. They play two key roles - one of setting up and configuring the Application for the Organization's needs and the day-to-day upkeep and support to users.

Approval

Approvals are checks and balances put in place to ensure that an action has required authorization for implementation. Approvals ensure that the action being considered is thought through and any reactions are anticipated and planned for.

Approver

Approver is a contact who is authorized to allow or deny the requested action on a request. Approvers are required to give their approval to a request before the request can be processed.

Approval Phase

A Change ticket can be processed through multiple levels of approval (Multi-Level Approval). For example, technical approval, financial approval, etc. Approval Phase can be used to identify which level of the Approval Process the ticket is currently at.

Attachments

Attachment is a document or file that could provide more information related to the Request. The Attachments area of the Submit Request Form allows the user to add attachments to the Request. The user can attach any document related to the Request or can be of use to Support in responding to the Request by specifying a file path.

Attachments can also be associated with Contact Records, Solution Records, and Configuration Item Records.

Attributes

Attributes refers to the properties or characteristics associated with Configuration Items. For example, Make, Model, Manufacturer, Manufacturing Date, Warranty dates, etc. could be attributes of an IT object. Each Attribute has a value (which may or may not be unique). Depending on the type of Attribute, the Attribute value could be a number, alpha numeric text, or plain text.

Auto-Route

Auto Routing is an automatic mechanism to assign (route) a new ticket when it is saved first time. Auto-routes get applied on the basis of predefined rules or values of parameters of the tickets. Based on matching conditions specified for an auto route by the Administrator, a new ticket qualifies for the auto route. Set fields and action defined for auto route are executed. Auto-Routes can automatically assign a Request to an identified Support Group or an individual.

Average Rating

Users can submit feedback regarding usefulness of a Knowledge Article. They can also rate the Article on a scale of 1-5. The application calculates the average of rating submitted by different users and displays it as Average Rating on the Knowledge Article.

Base Metric

Base Metric refers to the Service Metric against which a Service Target is applied. Multiple Service Targets can be applied to a Service Metric.

Bulk Process

Bulk Process refers to the processing large quantity of data into the application. You can bulk import, update or even delete much of the preliminary records like organization records, contact records, support groups, roles, CCTI, and Configuration Items.

Business Hours

Business hours indicates the working hours of a support group. Multiple schedules can be associated with the support group. If no schedule is defined, the business hours of the support group is considered to be 24X7.

CAB

Change Advisory Boards (CAB) consist of groups of people who assist the Change Manager in planning, prioritization, risk assessment, and scheduling a Change. A CAB usually contains representation from all departments or entities associated or impacted by the Change.

Case ID

Case ID is the unique identification number given to a New ticket reported via Nimsoft Service Desk. Each time a new request is generated, a Case ID is generated. Any subsequent tickets created as a child out of this ticket will carry the same number as the parent ticket for easy reference and relationship tool. It is also possible to choose the option to having fixed Case ID based on ticket type using configuration parameter.

Categorization

Categorization is the process of logically grouping identified entities for a specific purpose. Nimsoft Service Desk allows Categorization of Tickets, Configuration Items, and Solutions.

Categorization in Nimsoft Service Desk has a four-tiered approach to define an entity. First tier is 'Class'; then, a 'Category' under that 'Class'; then, a 'Type' associated with the 'Category'; and finally, an 'Item' associated with the 'Type' selected. This is also referred to as CCTI which stands for Class, Category, Type, and Item as a method of categorizing Configuration Items in Nimsoft Service Desk.

Cause

Cause is a field in the Solutions Details section of tickets. An Incident or Problem occurs due to some reason, which is usually identified upon investigation of the Incident or Problem. This reason is referred to as the Cause.

Change Approval

ITSM recommends that all Change Requests pass through a Change Approval Process, wherein a competent person or a competent group studies the Change and considers the implications of the Change before a Change is implemented. This process of seeking permission to implement a Change is referred to as Change Approval.

Change Type

Change Type is a way of classifying a Change Request. A change can be classified as Normal, Standard, Break-Fix, Emergency; or by any other value you use to classify a change.

Classifying a Change by specifying Change Type enables you to configure workflows specific to a Change Type. You can also use Change Type as a Matching Condition for Auto-Routes, Action Options, and Approval Groups

CI Attribute Template

Attributes of a CI specify various aspects of the Configuration Items, like Make, Model, Warranty duration, etc. Standard attributes common to all Configuration Items are available as default attributes. CI Attribute template is a configurable template which you can use to capture additional attributes for a CI based on the CCTI of the CI.

Child Ticket

Child Ticket refers to a ticket that is created from another open ticket. A ticket logged in Nimsoft Service Desk can be classified as Service, Incident, Problem, or Change ticket based on the the nature of the request. Child Ticket can be created to classify a ticket differently or to work upon a ticket based on the different ticket type.

Client Note

Client Note is an option available to classify a worklog that is added to a ticket. When an SSU updates a worklog on an existing ticket, the worklog gets added as Client Note. Similarly, if the client has sent out any communication related to the ticket (via phone or email) and this needs to be appended to the ticket, it can be added as Client Note.

Client Viewable

Client Viewable is an option in tickets that allow the Worklog to be visible to the requestor. Client Viewable Worklogs contains input and details that could be of interest to the requestor. The user can mark a Worklog as Client Viewable.

Configuration Items

Any component of an IT Infrastructure is referred to as Configuration Item (CI). IT components like Hardware, Software Applications, Network devices, documentation, etc. are examples of Configuration Items. Records of Configuration Items, including a history of all actions on a Configuration Item can be maintained in Nimsoft Service Desk.

Communication Templates

Communication Template is a pre-configured Email template made available by the Administrator. Communication Templates can be made available for sending manual communication from the ticket. Communication Templates can also be attached to auto-routes, ticket action-options, approvals, etc. and can go out as Automatic Notifications when an associated action is taken on the ticket.

Contact Records

Contact Record refers to the details of a Contact stored in Nimsoft Service Desk. Besides basic contact details, the Contact Record also lists the Organization, Site and Location details of the Contact and indicates which group(s) the Contact is associated with. Action like having access to login to Nimsoft Service Desk, being part of approval process, receiving service feedback forms, etc. are also controlled from the Contact Record.

Contextual Approver

Contextual Approvers or Contextual Reviewers indicate that the name of the Approver or Reviewer will be selected from the context of the ticket.

For example, consider a Standard request for a Change (like access to some material or a site on the internet), that does not need an elaborate Approval process. For such changes, you may require Approval from the Requester's manager.

Created Date

Created Date refers to the date the entity was created in Nimsoft Service Desk. Created date can be found on tickets, Configuration Item records, Contact Records, Solution Records, and Reports in Nimsoft Service Desk.

Custom Fields

Processing of a ticket may call for Additional Fields in a ticket over and above the standard common fields provided by the Application. Such fields that are configured for a given ticket type are called Custom Fields. You can configure Custom Fields template for a ticket and relate it to the CCTI of a ticket. When a ticket with the identified CCTI is created, the Custom Fields gets applied on the ticket.

Custom fields are visible from the Additional Information tab of the ticket.

Dashboard

A Dashboard is a user interface that integrates and presents required information generally in graphics mode in an easy to read way. Dashboards are interactive displays that allow the user to drill down to details on the information presented.

Defined Searches

Defined Searches refers to a search executed against a pre-configured SQL query, where specifics of a search are listed. Defined Searches can be used for frequently used searches and also are a pre-requisite for configuring charts.

Deputy

A Deputy or Delegate is a person you have nominated as an alternate contact when you are out of office. Nimsoft Service Desk diverts notifications meant for you to your deputy when you are out of office. A contact nominated as Deputy can take up activities like Approving a Change when you are out of office.

Dependent Data

Data where an entity is used and was linked by manually configured relationship. Dependent Data is listed on "Dependent Data" tab for Organization, contacts and configuration Items. Dependent Data displays a list of dependent entities, their description, the action on termination, and the "Number of records" for each. This information is important when an entity has to be unrelated manually before its associated organization is terminated.

Direct URL

Direct URL refers to the clickable links which directly take you to a given record or form from an email received from Nimsoft Service Desk. Direct URL to the appropriate forms are also sent via Email as part of notification for approvals or service.

Database Server

The database server name identifies the database server to client applications. In most cases, you can choose the default value. The database server name that you specify is the value for the DBSERVERNAME configuration parameter.

Database Server Port

The database server port number specifies the port entry for the database server in the sqlhosts registry.

Database Schema

A database schema of a database system is its structure described in a formal language supported by the database management system (DBMS) and refers to the organization of data to create a blueprint of how a database will be constructed.

Draft State

Draft State refers to the state of a Solution in the Solutions Knowledgebase. When a solution is added to the Knowledgebase, it has to be first approved by a competent person before the solution is made available for use. A solution before it is approved lies in the Draft State. In this state, the solution will not be available for use when agents Search Solutions for a ticket.

Dropdown List

Some fields in the Nimsoft Service Desk forms require the user to select one out of a fixed set of alternatives, for example, Priority or Urgency of a Request. The items that are available for the user to make One Fixed Choice from are made available in a Dropdown list. A dropdown list is indicated by an icon with a single downward pointing arrow at the end of a field box.

End Users

End Users refer to the users of IT in an organization. This could be people in different hierarchical positions in the organization who use IT to perform their day-to-day tasks. End Users may or may not be having access to the Self-Service User Interface of Nimsoft Service Desk.

Environments Affected

All IT objects that provide service to one particular kind of activity can be grouped into one environment. For example, an organization may have Production Environment, Testing Environment, Training Environment, etc. A Change that is proposed could affect any one or more environments. Information related to the Environments Affected can be documented using the Environments Affected field of the Change ticket.

Enable Login

The Enable Login checkbox allows you to indicate whether a contact will access Service Desk application or not. If the Enable Login checkbox is checked, the contact has to be assigned an appropriate license and system login id has to be created.

Escalation

Moving a Request to a higher level of the support structure is referred to as Escalation. This is done either when a Request cannot be handled by a lower level Support Group or when it requires specific inputs from a specific Support Group.

Fixed License

A Fixed license allows only an identified user to access the application at a time. A contact assigned a fixed license can access the application at any time.

Floater License

A Floater license is a concurrent user license, which allows a specified number of users to access the license at a specific time. The license is not tied down to a specific contact. It is bound only by number. If the available floater licenses are used up no additional users will be able to access the application till a logged in user ends the session.

Function

Function is a field in the Configuration Item record which indicates what a given Configuration Item is used for. This helps identify a Configuration Item better and helps particularly when a CI is part of a service.

Global Attachment

Global Attachment refers to a file that can be made available for use in other tickets logged in Nimsoft Service Desk. The file is also available for use as attachment in some other Nimsoft Service Desk entities (such as solution) in addition to tickets. When uploading an attachment, the user can mark an attachment as Global Attachment.

Global Issue

An Incident or a Problem is designated as a Global issue when it represents a group of similar Service Requests or Incidents. When the Global issue is addressed and resolved the other tickets also get addressed. When a Global ticket is resolved or closed, the status and reason codes for tickets related to it are also updated. The solution applied to the Global Ticket is also applied and associated with the related tickets.

Global Search

Global Search is a feature in Nimsoft Service Desk that allows the logged in user to search for records stored in the user's instance of Nimsoft Service Desk. Global Search executes a search for records from across ticket records, CI records, Contact records, and Solution records relevant to the search input.

Holiday list

Holiday List refers to the known holidays for a calendar year. Holiday Lists can be associated with Support Group Business Hours, Service Availability, SLA monitors, and Auto-Routes.

Inactive

This indicates that the entity is not usable for transactions by Nimsoft Service Desk. An organization, contact, CI, template, etc. that is marked as Inactive cannot be used for any transaction in Nimsoft Service Desk. An Inactive entity cannot be related to an Active entity in Nimsoft Service Desk. For example, an Inactive Configuration Item cannot be related to an Active Configuration Item.

Import Logs

Import logs refer to the logs generated when Bulk Upload is in process. Details of the record uploaded, an error encountered when importing the record, severity of the error etc. can be identified from the Import Logs.

Import Sheet

The Import Sheet is visible during the Bulk Upload process. The import sheet displays a list of records to be imported in a given worksheet; mapped in a tabular manner.

Incident

An Incident refers to any unplanned interruption of an IT Service or deterioration in quality of Service available to the end user. Loss of Internet connectivity or slow response time are examples of an incident.

Knowledge Base

Nimsoft Service Desk allows users to create and store articles related to solutions for tickets, news, FAQs, Known Outages. Such information that is useful for Self-Service Users and Service Desk Agents can be stored in the Knowledge. Users can access articles in the Knowledge Base based on permissions assigned to the article.

Knowledge Article

Knowledge Article or KB Article refers to an item in the Knowledge Base. The Knowledge Article could either be a solution to an incident that has previously occurred, or other incidents that may occur in the IT Objects with steps to resolve the incident.

It could also be informative articles on how to use an IT Object or service or other such useful information. Users can access Knowledge Articles in the Knowledge Base depending on the permissions given by the Administrator

Keywords

Keywords are significant terms, words, or phrases that capture the essence of a text. They are used in searching through computerized information by matching keywords given by user with keywords for the item being searched. Keywords can be used to search for Matching Solutions from the Solutions Knowledge base.

Known Outages

An interruption in availability of a system or service is known as an Outage. The Known Outages link under Support Services displays a list of all Planned and Known Outages or unavailability of an IT object or service. Publishing this information allows the user to be aware of any service unavailability and plan their work accordingly.

Landing Page

Landing Page refers to the page that is displayed when a user logs into the application. By default, the Landing Page is the List Tickets screen in the Home Section. Nimsoft Service Desk allows users to choose their own Landing Page as different from the default.

License Type

License type refers to the type of license assigned to a user. A user can be given Fixed license, Floater license, Self-Service or Web-Services license.

Location

Location indicates the lowest level in a three level hierarchy of organizational unit in Nimsoft Service Desk below a Site in Nimsoft Service Desk. A Site can have multiple Locations.

Locations Affected

In large organizations with several locations, a proposed Change could impact one or more locations. This information can also be captured when planning a Change. Details of Locations Affected can be captured in the Location Affected field in the Change Ticket.

Locked Tickets

Locked Ticket refers to the state of a ticket which does not allow modification of any field except the worklog field. A ticket gets locked when a ticket form is open and is being worked upon. This ensures that a ticket is not getting modified simultaneously by more than one person. If configured accordingly, a ticket can also be locked with it is in the approval process.

Look-Up

Look-Up refers to a list of records or entities from which user can select one or more to associate with the currently open record such as a Ticket or CI etc. Some Lookups also have search and filter features. Some frequently used Look-Ups are associated with name search, solution search, CI search, Attachment Search, etc.

License Key

License Key is a system generated code that is used to renew or add licenses.

Matching Conditions

Some workflow items such as Auto routes, Action Options, etc. are applied to Service Desk tickets based on the specifics of a Ticket. These specifics are captured as Matching Conditions in form of Fields and their values while defining the entity (Auto Route , Action Options).

Navigation Menu

The right side pane of the Nimsoft Service Desk Application which contains the modules of Nimsoft Service Desk and links to the action under each module is called the Navigation Menu.

Notifications

Notification refers to the communication sent from the ticket intimating the recipient regarding an action that has been taken on a ticket. Notification can be sent on ticket assignment, SLA threshold violation, ticket resolution, etc.

Operating Level Agreement

Internal agreements between different internal departments of the support organization regarding terms of service, priorities, conditions, etc. are called Operational Level Agreements (OLAs). Usually an organization will set up a series of OLAs internally to meet an SLA externally.

Organization

Organization is the detail of the customer's company - its vendors, supplies, support providers, etc. maintained in Nimsoft Service Desk. A customer slice may have more than one Organization record.

Outstanding Approvals

Outstanding Approvals allows the viewing of all the tasks that are pending approval or review. Users can see a list of tickets pending approval or review and click on any ticket to view its details.

Outage

A failure or interruption in the availability or functioning of a service is called an Outage. An Outage could result due to a sudden failure or non-availability of a service or an outage could be caused due to a planned maintenance or change.

Parent Ticket

A Ticket can be related to other tickets in Nimsoft Service Desk. When one ticket is created from another ticket using a workflow action option; the newly created ticket becomes the Child Ticket and the older ticket is the Parent Ticket. Action from a parent ticket can be applied to a child ticket; and similarly, action on a child ticket can be applied to the Parent Ticket.

Parameter Value

Parameter value refers to the value set for a Configuration Parameter. You can choose from available options that will be available as radio buttons or drop down lists; or specify a value for a free text field.

Password Strength

This defines the complexity and strength of passwords. It is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. It can be configured at different levels from 1 to 4 to reflect the complexity and strength.

Permissions

Permission refers to the authority to do some action or see an option in Nimsoft Service Desk. The Administrator manages permissions for a range of actions available to the agents and Self-Service Users.

Phase

Phase is associated with tickets in Nimsoft Service Desk. It allows segmentation of the Workflow actions. It is used to define the steps in a given process workflow. The default configuration of Nimsoft Service Desk defines some actions that transition tickets through phases, and others that transition tickets within a phase.

PIN Authentication

PIN Authentication refers to the practice of using some mode of authenticating a user. This is needed when caller authentication is merited by the nature of the request.

Predefined Searches

Predefined Search refers to a list of pre-configured queries that have been made available by the Administrator. Predefined Searches are created for enabling an easy search for information that agents frequently need to search for. Predefined Searches also form a background for reports that can be generated from the different modules.

Primary Group

A user can be member of several support groups; based on the nature of requests handled. Primary Group of the user indicates the main group that the user is associated with. While a user will be able to inherit permissions granted to all support groups that he/she is part of, actions like participation in Service Feedback etc., are controlled by the Primary Group. Only one group can be set as Primary Group.

Primary Organization

A contact can be related to multiple organizations, but only one organization can be marked as Primary. The Primary Organization of a contact controls aspects of the contacts interaction with the application like participation in Service Feedback, Contact Status etc.

Priority

Priority refers to the act of prioritizing the ticket depending on the Severity, Impact or Urgency of an Issue reported by the requester. By prioritizing the ticket appropriately ticket can be queued and resolved effectively.

Process

Process is a structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the roles, responsibilities, and tools and management control required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed.

Nimsoft Service Desk automates the workflow steps required to accomplish the structured set of activities associated with a given ITIL Process.

Problem

An unknown underlying cause of an Incident which causes the Incident to reoccur is termed as Problem. A problem has a root cause, which needs to be identified and corrected to prevent the problem from having larger consequences.

Reason Code

The Reason Code is associated with the Status and indicates why the entity is in a particular Status. For example, a Change ticket may be in the "Queued" Status and its Reason Code could be "Auto-Routed".

Recurrence Pattern

Recurrence Pattern relates to schedules where some patterns for repetition is to be set. It controls the frequency of occurrence of the target activity. Recurrence pattern can be configured for Scheduled Activities and Service Feedback Schedules. Frequency of occurrence can also be set for Schedules (Service Hours, Business Hours).

Relation Domain

Relationship Domain indicates the nature of relationship between related Configuration Items. The relationship could be logical, network, power, or service.

Relationship Type

Relationship Type refers to how one Configuration Item is related to another within a given Relationship Domain. Type could be parent - child relationship in a logical domain or upstream of, downstream of in a network domain. This allows visualizing how the CIs relate to each other.

Relationship Graph

Relationship Graph indicates the graphical representation of how two or more Configuration Items are related to each other. The Relationship Graph shows the relation between Configuration Items within a Relationship Domain.

Requester

Requester is the person who is requesting for the service - either for self or for someone else. The Requester field contains basic contact details of the person who has requested for the support or service.

Resolution

Resolution can refer to either ways to resolve an incident to restore service; or steps to overcome some issue being faced by the user. It can also refer to the final step towards providing a service requested for by the end-user. Tickets need to be progressed towards resolution through different actions to service the request.

The Resolved status is set on Service Desk tickets when the request / issue /error has been removed from the infrastructure. Some tickets are set to auto-close in a specific number of days after transition to “Resolved” status. Others are set (based on priority by default) to require the user or agent to actively close the ticket, generally after verifying with the Requester.

Required Fields

Required Fields are those fields in the Ticket forms where it is compulsory for you to fill in appropriate values before submitting the request or while making changes to an existing request. The fields that are to be marked as Required Fields are chosen by your Application Administrator. All required fields are marked by a Red Asterisk.

Resolution Time

Resolution Time indicates the time taken to resolve the ticket thereby changing the status of the ticket from Active to Resolved. Resolution time can be used as a measure to apply SLA Compliance monitoring.

Resolved

The Resolved status is set on Problem tickets when the error has been removed from the infrastructure. Some tickets are set to auto-close in a specific number of days. Others are set (based on priority by default) to require the user to actively close the ticket.

Response Time

Response time indicates the time taken to accept assignment of a ticket and thereby change the status of the ticket from New to Active. Response time can be used as a measure to apply SLA Compliance monitoring. Internally for OLAs, Response time can also be considered when a ticket is reassigned to another group and the how quickly the group responds to the escalated ticket.

Request Fulfillment

Request Fulfillment is the process of dealing with Service Requests from the users. The objectives of the Request Fulfillment process include-

- Providing channel for users to request and receive standard services for which a pre-defined approval and qualification process exists
- Providing information to users and customers about the availability of services and the procedure for obtaining them
- Providing and deliver the components of requested standard services (e.g. licenses and software media)
- Providing with general information, complaints or comments

Reviewer

A Reviewer is a contact who is consulted about a proposed change. A reviewer has no authority to allow or stall the Change Approval Process, but the views of a reviewer are considered while deciding about a change.

Risk Assessment

Any change that is to be implemented carries the chance of some risk of failure or disruption of an existing system or service. It is therefore necessary to carry out adequate Risk Assessment prior to taking up a Change.

Nimsoft Service Desk therefore provides for the ability to record the result of Risk Assessment for a Change Request setting the risk level as Slight/Negligible, Notable, Minimal or Significant. Risk Assessment should lead to taking risk mitigation measures before hand.

Roles

Roles are used for inheriting permissions in Nimsoft Service Desk. Contacts plus Groups can be related to a Role to pass down permissions assigned to a Role. One person or team may have multiple Roles. For example, the Role of Configuration Manager and Change Manager may be carried out by a single person.

Roles in Nimsoft Service Desk define the level of access/actions available to agents within Nimsoft Service Desk. The Nimsoft Service Desk default Role configuration is designed to roughly map to the typical process roles in ITIL.

Routing

Nimsoft Service Desk allows automation of assignment of tickets, communication from tickets, and identified action on tickets, using workflow tools configured based on Matching Conditions. These automatic actions are carried out by the Routing Engine.

Report Database Server

A report server is a stateless server that uses the SQL Server Database Engine to store report metadata and object definitions.

Report Database Server Port

The report database server port number specifies the port entry for the report database server in the sqlhosts registry.

Schedules

Details of when a task or activity is to be carried out can be fixed by a Schedule. In Nimsoft Service Desk, Schedules can be attached to Auto-Routes, SLA Targets, service availability and group availability. Schedule also refers to schedules created by administrator for automation of ticket creation for repetitive tasks based on needs of Schedule owners using Manage Schedules module.

Self-Service Users

Users who have limited interaction with the Application and therefore need only limited features and options are called Self-Service Users. In Nimsoft Service Desk, besides logging and tracking own Requests, the Self-Service User can view Requests that require his Approval or Review. Self-Service Users also have access to a limited number of simple solutions from Knowledge Base.

Service Desk

Service Desk is the organizational unit that acts as a central/ single point of contact between service providers and users of the services on a day-to-day basis. It is also a focal point for requesting standard services and reporting Incidents.

Service Desk Agents

Resources, who are part of the IT Support Team in an organization and are involved in providing IT support and services are called Service Desk Agents. They are mainly the providers of IT Support and Service to the end users (the Self-Service Users) of IT in an organization.

Service Feedback

Service Feedback is the process of soliciting feedback from the end users of support for qualitative aspects of the service provided. Seeking Service Feedback allows you to manage the quality of service offered by the Service Desk or the Support organization.

Service Feedback Schedule

Service Feedback forms are sent to chosen participants configured on a Service Feedback Schedule. As per the schedule, participants receive notification about the feedback from being sent out. A schedule can be configured as Anonymous, and a recurrence pattern can be associated with the schedule.

Service Hours

Service Hours refers to the Schedule configured for a Configuration Item. You can configure multiple schedules for a CI, like Availability Schedule and Maintenance Schedule.

Service Level Agreement

Formal agreement between the users of IT Support and the IT Support providers in terms of the level of support and an understanding about availability, priorities, conditions, guarantee, etc. are called Service Level Agreements (SLAs). SLAs are formal or informal negotiated agreements between the Service Provider and the customer regarding the terms of service.

Set Fields

Set fields is a feature available to the Application Administrator while configuring Action Options, Auto-Routes or Approval Groups for managing the workflow on a ticket. The Application Administrator can select the attribute(s) and specify what value each attribute should assume after the execution of the Action Option or Auto Route or a step of change Approval Process.

Service Metrics

A metric is a well-defined way to measure and quantify something of interest. A set of Metrics form a system of related measures that enables quantification of an identified characteristic against a given set of values. In Nimsoft Service Desk, there are 18 pre-defined Service Metrics Measuring "Time" as a unit of Service Quality. These 18 Metrics act as measures of SLA Compliance for tickets. (Also see SLA Compliance)

Service Request

Request from a user for information, advice, or access to a regular IT service or standard change like resetting password or new user are classified as Service Requests. Issues faced by End users while availing IT services can also be reported through a Service Request.

Service Targets

Service Targets are applied to Ticket management activities of Service Desk, using Service Metrics to monitor SLA Compliance. Individual Targets can be defined for tickets based on Matching conditions like Ticket Type, CCTI,, affected service, Assigned To group etc. Matching conditions are used to identify Requests to which the Target is applicable. Further, time thresholds must be attached to the Service Targets to measure SLA Compliance of a Request.

Severity

Severity is a way of defining how debilitating an Incident is. If an Incident is causing breakdown in the normal functioning and is causing stoppage of work, the severity can be considered as major. This field will be available on Incident and Problem tickets.

Site

Site is used to depict either geographical or functional distribution of an Organization in Nimsoft Service Desk. An Organization can have multiple Sites.

SLA Compliance

SLA Compliance indicates whether the terms of formal agreement with the customer in terms of response and resolution of a request have been met or not. By defining Service Targets based on appropriate Service Metrics, and applying then to ticket processing activities, it is possible to monitor whether an SLAs are missed or met.

Session

A Session refers to an instance when a user accesses the application. A session is recorded when a user logs into the application. The session remains active till the user logs out of the application or is logged out by the application by an external input.

Slice

Slice refers to one instance of the application which is specific to a particular customer. All transactions and records related to that customer are maintained on that slice.

Session Timeout

This specifies the number of minutes that a session can remain idle before the server terminates it automatically.

Configuration Parameters

Several features of Nimsoft Service Desk can be turned on or off, or modified to some extent. Configuration Parameters allows you to manage the feature or functionality of the application as per your organizational needs.

Sort Order

Sort Order is a numeric value that indicates the order or precedence or appearance of a record in the application. Sort Order appears in several administrative forms, particularly where sequencing of the entity or record becomes important.

Stakeholders

Stakeholder refers to all the people who are involved with a particular activity or ticket and who in one way or the other are to be informed about any activity on a ticket.

For example, stakeholders for an Incident Ticket could be the person reporting the Incident, the person experiencing the Incident, the group to whom the Incident Ticket is assigned, and the supervisor or manager of the group owing the ticket. All stakeholders need to be kept updated about activities on a ticket they are involved in.

State

State is associated with Knowledge Articles and Service Feedback forms. It indicates whether the form is complete, has been reviewed and whether the form can be used for association with other related transactional records or not.

A Knowledge Article can be in Draft or Approved State and a Service Feedback form can be in Draft or Published state.

Status

Status is associated with all records maintained in Nimsoft Service Desk. It indicates whether an entity or record is available for use for transactions in the application or not. The status of a record can be Active or Inactive.

Only Active records are listed in lookups used for associating one entity with another. An inactive record will not be visible in the lists and will not initiate or trigger any automatic action.

You can search for Inactive records by applying filter to view inactive records.

Standard Change

Where a Change is part of routine operations, for example adding new users to a system, provisioning additional systems for new recruits to the organization, etc., the Change can be implemented without much assessment or analysis. Such a Change is classified as Standard.

Support Groups

Support Groups are used to bring together Contacts either by their specialization, by their physical location and working hours, or by the action they perform in Support. A Contact can be member of multiple groups.

Support Services

Support Services refers to the services provided to the end users of IT Services in an organization. Support Services include services such as responding to queries relating to how to utilize an IT service, responding to reports of service unavailability or quality drop, and activities undertaken to ensure that IT Services are available to end users when the services are needed.

Survey Forms

Survey forms are service feedback questionnaires that are sent to end-users of support. The survey forms are sent to end users to solicit feedback on service satisfaction on identified parameters.

Symptom

This field appears on the Incident and Problem ticket and the associated solutions database, to capture the visible and directly experienced aspects of an issue.

System User ID

System User ID is the unique identification assigned to a contact who has been granted access to the application and an associated license. System User ID has to be unique; and no two contacts can have the same System User ID.

Take an Action

Take an Action link in the Ticket Toolbar refers link that displays all the Action Options that a user can apply to to process a ticket during work flow such as change the Status and/or Reason Code of a ticket. The Take an Action option contains only those actions that can be taken on a ticket when it is in a particular state (status and phase).

Task

Task refers to Task Tickets that can be created for delegating / assigning to different resources towards activities of fulfillment, Diagnosis, Investigation, Change evaluation, Implementation and completion of an open ticket. Task Tickets enable effective work breakdown by identifying individual Tasks that need to be done towards a larger activity. They also provide an ability to assign activities to different resources.

Task Flow

Task Flow refers to a collection of Task Group(s) and/or single tasks created for completion of any activity like standard change implementation. The Administrator sets up a Task Flow where activities are to be done in a specified sequence; or simultaneously; but in a known order.

All task tickets related to a task flow are not created simultaneously; rather the administrator sets up the action to be taken on a task when it is completed successfully; and if it fails. Depending on whether a task in the flow is successful or it fails; the next action is determined or next task ticket is fired.

Task Group

Task Group refers to a collection of Tasks that need to be done to implement activities related to a ticket; like implementation of a standard change. The Administrator sets up Task Groups as a collection of all tasks to be done towards a particular planned activity. When working on a Ticket where a given set of tasks need to be done; the user can create all task tickets related to that task group using that Task Group Template.

Task Information Tab

The task Information Tab on a ticket contains details of the Task Tickets that have been created related to the main (Parent) ticket. The Task Information tab appears on the ticket after the ticket is logged and a ticket number is generated for the ticket.

Task Order

Task Order is a field on the Task Ticket Form, which allows the user to sequence Tasks Ticket that are related to the same larger activity. If there are five Tasks to be done towards a Change ticket, then each Task can be executed in a given sequence. This allows organization of the Tasks to complete any activity in a synchronized way.

Task Templates

Task Template refers to the ticket template create for Task Tickets. Task Templates can have additional features like Auto-Assign Action and Auto-Assign on Create associated with it.

Threshold

Threshold is the tolerance limit at which a pre-defined action sets off. In Nimsoft Service Desk, time thresholds are associated to Service Targets to measure SLA Compliance.

Terminate Organization

Terminate an organization is to remove all data relating to the an organization from Service Desk application using the Terminate button. However, removal of a specific organization from the application is based on data dependencies and existing relationships. Before terminating the organization, you should unlink any transaction data from the organization and unrelate any dependent data that is required elsewhere in the application. Any entity attached to a terminated organization also gets deleted from the application.

Ticket

A Ticket is a transaction document that records all the information related to a Request. It forms a basic entity in Trouble Ticketing, Issue Tracking, and Service Desk Applications like Nimsoft Service Desk. All requests submitted to the Service Desk or Support Organization are logged and tracked via tickets logged and updated.

Tickets Assignment

Tickets Assignment refers to moving the ticket to a particular group or individual's queue for action on the ticket. Ticket Assignment can be done by the routing engine via an Auto-Route or manually by an agent.

Ticket Classification

Categorization or Classification assists in grouping similar entities together in a logical way. Ticket Classification refers to the categorization applied to classify a ticket. You can choose an appropriate CCTI categorization from an available list to classify a ticket.

Ticket Life Cycle

Ticket Life Cycle refers to the progression of a ticket through different statuses from the time it is logged to the time it is closed. The ticket progresses in its life cycle based on the work done on the ticket.

Ticket List

Ticket List refers to a list of all open tickets in the queue of a logged in user. The Ticket List displays a list of all tickets assigned to the logged in user or his/her support group(s).

Ticket Locks

Ticket locks are used to indicate that the issue is being worked upon by someone else or it is not to be modified due to some reason. In Nimsoft Service Desk, a locked ticket can be identified by a lock icon that appears alongside the ticket description in the ticket list.

Ticket Status

Ticket Status is used to specify which stage of the life-cycle the ticket is currently at. Ticket moves through different statuses from the time a request from a customer is logged as a ticket, till the time the ticket is resolved/ closed. The values for ticket status are fixed, however, a ticket can transition from one status to another and back depending on the workflow configurations and actions taken on the ticket.

Ticket Templates

Ticket templates can be configured by the Administrator with details of common, standard requests. Ticket Templates have a pre-designed format in which all required details are identified and populated into the request automatically. Administrator can configure Ticket Templates for all type of tickets and can manage their use by applying permissions.

Ticket Toolbar

The Ticket Toolbar is the Menu Bar on the ticket which lists all possible actions that can be done on a ticket. The Ticket Toolbar lists actions like creating a new ticket, copying to new ticket, printing a ticket, managing ticket status, etc. The exact links on the Ticket Toolbar are controlled by your Administrator.

Ticket type

Ticket Type refers to whether the given ticket is classified as a Service Request, Incident, Problem, Change, or Task Ticket. The Ticket Type determines things like assignment of a ticket, SLAs applied to a ticket, etc.

Time Zone

A Time-zone refers to a region on Earth, bounded more or less by the lines of the longitude, that has a uniform, legally mandated Standard Time. In globalized economies, IT Service Management may involve situations where the Service Users and Service Support Groups are situated around the world in different countries and in varying time zones.

Nimsoft Service Desk, therefore, takes into account the Time Zone of the logged in user and performs the necessary time conversions to user's time zone for displaying time related information. Time Zone information can also be associated with Auto-routes, Service Availability, and SLA Calculations.

Underpinning Contract

An Underpinning Contract is an agreement between the IT Support organization and the external service provider (third party). An Underpinning Contract supports achievement of The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.

Used For

This field which appears on the Support Group record identifies what a support group can be used for. You can choose one or all of the check boxes, Permission, Notification, Assignment, Approval and SLA Escalation

Users

A user is a contact who has been granted access to the application. This means that login for the contact is enabled, and the contact has a license to access the application

Values

Attributes have values that specify details about the attribute. A value could be alpha numeric text, a number, date & time, an option selected from a dropdown, multiple options chosen from a look up list, etc.

Violation Threshold

Threshold is the tolerance limit at which a pre-defined action sets off. Multiple Thresholds can be configured for a Service Target; which work together towards monitoring the compliance towards a Service Level Agreement. A Violation Threshold indicates that at this value, the SLA has been breached. A Service Target can have only one Violation Threshold.

VIP Users

VIP Users in Nimsoft Service Desk are Contacts marked by your Administrator as high priority Contacts. Their tickets are to be handled differently. A message indicating that the user is a VIP User is flashed when that Contact is selected as Requester of a ticket.

Workflow

The set of business steps required to execute a process. Most process policy/procedures describe the workflow to achieve the underlying process activities defined in a process. Nimsoft Service Desk implements workflow through a combination of Ticket Templates, Workflow Actions, and Auto Routes.

Workflow Actions

The Nimsoft Service Desk actions which can be executed, based on business rules/matching conditions associated with ticket types. The combination of Workflow Actions associated with a ticket type defines the workflow for that process.

Worklog

Worklog refers to the manual update made into the ticket for adding information that is significant to the request, but which is not directly captured by the application. Worklogs are usually added by Service Desk Agents who work on the ticket. However, worklogs can also be added by the ticket requester from the Self-Service User interface.

Appendix A: Licensing Information

Liferay

This product contains components of the Liferay Portal, subject to the following terms.

Copyright (c) 2009 Liferay, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The Above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS-IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USER OR OTHER DEALINGS IN THE SOFTWARE".