Ticket Handling and Related Concepts

This article contains the following topics:

- Ticket Management Process
- Ticket and Ticket Lifecycle
- Ticket Types
- Auto-Routes and Workflow Actions
- Change Types and Change Approval
- Configuration Items and Affected Services
- Ticket Relationships
- SLA Compliance Monitoring
- Knowledge Articles and Knowledge Base
- Support Groups and Roles
- Organization and Organization Based Security

As an analyst you work extensively with tickets. Besides working on a requested service, you can take multiple actions on a ticket. You can reclassify a ticket that is based on the nature of its request. You can determine the progress of the request, update solution details to the ticket, and more.

As an analyst, you must to have a general understanding of ticket management concepts. This article provides the high-level concepts that are related to ticket handling in CA Nimsoft Service Desk.

Ticket Management Process

You can log new requests by sending an email to the designated support ID or from the application user interface. You can log requests by using a relevant catalog item from the Request Catalog or using the Create New option. Requests get auto-routed to different support groups based on the following criteria:

- Nature of the request
- How the request was created
- Routing rules

The administrator manages and controls the permissions and workflow actions available to you. Based on the request or issue you can create an incident, problem, change, or service request. You can also create a ticket of a different ticket type from an existing ticket. The outcome is to ensure that the request is handled using appropriate processes within agreed upon service delivery agreements.

Ticket and Ticket Lifecycle

A ticket is a transaction document that records all the information that is related to a request. The ticket fields contain information that is required to understand and fulfill the request from the end user. The administrator can configure and add custom fields to be available on the ticket and is based on the ticket categorization. Once, a ticket is created; it gets assigned to a support group. The administrator configures the assignment rules. The three main aspects of ticket progression, which are used when building the workflow process are:

**Phase:** During a ticket lifecycle, the ticket passes through different phases. Based on its progression the ticket can loop back to a previous phase. The phase definitions differ based on the ticket type.

**Status:** Status refers to the current stage of the ticket in its lifecycle. They can be New, Queued, Active, Pending, Complete, Resolved, Closed. Fixed ticket statuses cannot be modified. A ticket can move from one status to another - not necessarily in a specific order.

**Reason Code:** Reason code is used to assign a reason why a ticket is in a given status or phase. For example, a ticket could be set into pending status for several reasons - like Pending Customer, Pending Vendor, Pending Information.

A combination of the ticket status and reason code is used to manage the workflow actions available and manage the ticket progression. As a ticket progresses it grows to include activities toward resolving, fulfilling, and closing the request. Ticket progression also includes manual, automatic actions, and communications to and from the ticket. The administrator can configure different workflow actions to be available on the ticket to control the progression of the ticket.

Ticket Types

In CA Nimsoft Service Desk there are five types of tickets:

**Service Request:**
A Service Request is logs and manages standard requests for information or access to systems and services. Service requests are handled using service request management workflow processes and is monitored for SLA compliance. For example, an end user seeks information about how to set up and configure work emails for mobile devices.
Incident Ticket:
An Incident Ticket is used to report and manage issues like a disruption, unavailability, reduction in the quality of a system or service. The Incident tickets are handled using incident management workflow processes. The response and resolution of these tickets is monitored for SLA compliance. For example, a request is logged when the end user is unable to send or receive emails from the cellphone. This service is typically available to the requester; and the service has been disrupted. Identify the cause of service disruption, restore the service quickly, and communicate with the requester about the resolution.

Problem Ticket:
A Problem Ticket is used to investigate, resolve, or mitigate major issues affecting many users. The problem tickets are handled using problem management workflow processes. Generally, root-cause analysis and resolution take time; and these tickets could or could not be monitored for SLA compliance.

Change Request:
A Change Request is used to log and manage a request for change to the IT Infrastructure or services. Some changes could affect only the requester (or a small group of users); while others affect many users. All change requests go through a change approval process. Based on the nature of the change, the approval process varies and is handled using the change management workflow processes. A change request could be monitored for SLA compliance. The time that is required to respond and resolve a change is based on factors like getting an approval.

Task Ticket:
Tasks Tickets are used to track and manage smaller units of work toward the completion of another ticket. A Task ticket is logged as a child to another ticket. A Task Ticket is usually a Change or a Problem ticket. Each task can be handled either at a time by different people; or in a set sequence.

Auto-Routes and Workflow Actions
Auto-Routes are ticket routing rules that route newly created tickets to appropriate support group queues. Routing is based on matching conditions such as its source, priority CCTI.

The administrator manages and configures the workflow actions and auto-routes responsible for the progression and assignment of tickets. This progression and assignment of tickets is based on the request handling process that is defined for each ticket type.

Auto-Routes:
Auto-Routes are rules that route new tickets to appropriate support group queues based on matching conditions such as source and priority CCTI. Categorization by CCTI is also important to generate reports. Auto-routes sets values for fields like Phase, Status, and Reason Code. Some auto-routes have communication templates that are associated with it; and send out notifications when a ticket is created and assigned to relevant stakeholders.

Workflow Actions:
Workflow actions are a set of actions that can be taken on a ticket. When a workflow action is executed on the ticket, some field values are set as configured; and the ticket is moved to the next state. Workflow actions are specific to each ticket type and are an important aspect of the workflow design. Workflows are manual actions that are made available to analysts by assigning permissions to different support groups or roles. A workflow action is configured and available on a ticket that is based on matching conditions like Status, Reason Code, and Phase. Some workflow actions options are available without any matching conditions on a ticket in any state.

Workflow actions can also be configured to send out notifications to stakeholders. Some values can be set as required fields before execution of the workflow action. Some action options have associated special functions; which further automate the execution of an extra action (like Accept Assignment, Reassign).

The administrator controls the access and permissions to workflow actions. An action available to you could not be available to another analyst.

Change Types and Change Approval
Change is defined as an addition, modification, or removal of an existing IT system or service. Change could be part of software or hardware systems, configurations, access, and so on. A change can be reactive – in response to a problem or proactive – to prevent potential problems or improve service delivery. For example, adding or removing users from a system or group; or provisioning systems for a new hire.
Change request can be classified into the following four types:

**Standard Change:** This change type is suggested for common requests. For example, request from an employee for the installation of a software, or access to a system or database. A contextual approver or an approver that is associated with a configuration item approves such requests.

**Normal Change:** This type of change is suggested for implementing proactive, planned changes. For example, implementing new IT security systems which impacts how users access the IT resources over a VPN. Such a change would require a thorough investigation, detailed change implementation plans, multiple levels of review and approvals. Such a change requires potential down-time during implementation; and post implementation review implemented change.

**Emergency Change:** This type of change is suggested for reactive situations; where implementing a change is necessary to either correct or avert a major problem. For example, if a server is failing leading to downtime for several users the faulty server must be replaced. In, such situations a quicker approval and implementation process is necessary.

**Break-fix Change:** This type of change is typically used to report a change after implementation without an approval process. For example, if the security of a server was compromised, it must be removed from the network. A Break-fix change does not go through an approval process; and is only used to record the change.

The nature of a change is different and requires different types of approvals. Some changes need approval from a contextual approver like the manager of the requester; others require multiple approval levels. Sometimes you require approval from one or all approvers. Different approval types can be associated with a change ticket. The approval types that you can set are:

- **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 by rejecting the change.

- **Any One Approver:** A change is approved as soon as any ONE approver approves. The approval is rejected only when all the approvers reject the proposal.

- **Any One Approval or Rejection:** A single approver from the Approval Group rejects or approves a change. The decision of the FIRST approver who responds (Approve or Reject) to the approval process gets applied.

The administrator configures the rules for the approval of different types of changes and the approval groups that are associated with a change. In some cases, you can manually select approvers for a change.

**Configuration Items and Affected Services**

A configuration item is any component of an organization and its IT infrastructure. A CI manages and delivers an IT Service. For example, hardware, software, networking devices, peripherals, and documentation. CA Nimsoft Service Desk creates and manages a record of all configuration items in the organization. For example, mail hosts, servers, and client machines with essential software are required to deliver an email service. A record of all such services is created and saved as a CI in CA Nimsoft Service Desk.

A configuration item can be related to one or more configuration items in different relationship domains like logical, network, power, or service domain. This information can be used to troubleshoot any issues with the configuration item. When a ticket is logged to report an issue about a configuration item, the CI can be related to the ticket. Thus, building a history of all the incidents, problems, and changes that are related to the CI which can be stored and retrieved. If a ticket is logged to report issues with a service, the relevant CI can be related to the ticket as 'Affected Service'.

Contacts can be related to configuration items as Owner, User, Change Approver, Change Reviewer, and Support Provider. The contacts that are associated as Change Approver and Change Reviewer are used as contextual approvers for change tickets that are related to that CI. The status of a configuration item indicates whether the CI is in use or not. The status also specifies what stage of its lifecycle the CI is at. Configuration Items in all statuses except Deprovisioned is visible to analysts when relating a CI to a ticket.

**Ticket Relationships**

Ticket relationships refer to the different types of records that can be related to a ticket. Tickets can be related to other tickets or to configuration items. Attachments can also be related to provide more information.

**Ticket - Ticket Relationship:**

A ticket can be related to another ticket in the following three ways:

**Parent - Child Relationship:**

When, a new ticket is created from an existing ticket - the two tickets share a Parent-Child relationship. For example, if a change ticket is created from a problem ticket. A Task ticket is created only to complete units of work toward another existing ticket. A Task ticket is always logged as a Child ticket.

**Global Ticket Relationship:**
When smaller incidents are a result of a bigger issue, the ticket reporting the main issue can be marked as Global. Other incidents can be related to the global incident. For example, different users log several Incident tickets reporting loss of the connectivity. An incident is logged reporting that the network server has power issues, these issues are all due to the incident with the network server. Thus, resolving network server fixes the related incidents. Hence, the ticket that is logged for the network server can be marked as Global. You can relate all the other incidents to the ticket.

**Related Tickets:**

Tickets can also be related to each other for other reasons. For example, two tickets are logged for one CI. Resolving one ticket does or does not result in the resolution of the other ticket. Two tickets could be related to one another. The Relating tickets allow easy access and greater visibility for all issues that are connected to one configuration item.

**Ticket - Configuration Item Relationship:**

The configuration management database holds records of all IT systems and services. The IT support and service delivery teams support all the IT systems and services. The support team services tickets usually for issues or assistance with using a supported configuration item in the CMDB.

One or more configuration items can be related to a ticket when it is logged, or at any point in the ticket lifecycle. You can click a configuration item and can view its record details. You can view the relationship between a CI and a ticket by using the CI relationship graph.

**SLA Compliance Monitoring**

Service Level Management deals with the process of negotiating Service Level Agreements and ensuring that they are met. Service Level Management is ensures that all processes, agreements, and underpinning contracts are suitable for the agreed Service Level Targets. Service targets define the time that is allocated for a specified activity, are measured against set Service Metrics. A service target can have one or more threshold rules. One of the service targets can be set as Violation Threshold indicating that the SLA has been breached.

Factors like support group business hours and service availability govern SLA measurement. The SLA target progression icon displays the target status progression. The SLA target progression icon also indicates whether a ticket is approaching violation or violated the SLA target.

The administrator configures the threshold rules and the SLA monitoring of tickets. The administrator can also configure actions to be executed when a threshold rule is breached. Actions include sending notifications to different stakeholders or escalating the ticket to the next escalation group.

**Knowledge Articles and Knowledge Base**

Knowledge management deals with gathering, analyzing, and storing of knowledge and information within an organization. A knowledge article contains information about troubleshooting frequently occurring or previously reported incidents, instructions for setting up or configuring an IT service. Knowledge articles also contain news, solution details and about a supported system or services. Knowledge articles can be made available to users by assigning permissions to appropriate support groups or roles.

The knowledge base provides you with information about how to handle an Incident or problem that has previously occurred. The knowledge base can be used to expedite the issue resolution process and improve service delivery.

With the required permissions, you can also create knowledge articles. All new articles are created in the Draft state. Once created as a draft all knowledge base articles can be reviewed, refined, and set as Approved. Once approved, an article can be made available to different support groups or roles. You can also suggest solutions from tickets to be included in the knowledge base. The solutions items get added to the knowledge base in draft state.

**Support Groups and Roles**

A support group is a grouping of contacts according to their geographical locations, skill sets, or relative tasks that perform. Such a grouping of contacts is used for functions like skill-based ticket routing, ticket assignment, ticket approval. Support groups are used for actions such as notifications, permissions, approvals, SLA escalations, and assignment.

A role is a grouping of contacts and support groups that is based on the broader functions they perform. For example, the incident management role could be used to manage all functions that are related to incident management. Support groups providing L1, L2 (or higher) support and supervisors who manage teams of analysts could be under this role.

The administrator configures permissions like access to ticket templates, communication templates, workflow actions, knowledge articles. Permission is either given directly or by virtue of the support group the logged in User belongs to. A contact can be related to multiple support groups and roles. A contact inherits permissions that are assigned to each of the related support group or role.

A logged in user can access only those items that the user has permission to and that are in an Active state.
Organization and Organization Based Security

CA Nimsoft Service Desk supports three levels -- Organization- Site-Location hierarchy for managing Organization information. An organization can have multiple sites and each site can have multiple locations. Multiple organizations, with their own sites and locations, can be configured within the same instance of the application.

Users can be related to an organization, a site, or a location level in the hierarchy. While Users can be related to multiple organizations, one organization must be set as a Primary Organization for that user. Several features available to a logged in user like the ability to participate in service feedback, are managed at the organization level.

You can view tickets that users of different organizations log. However, the application administrator can enable organization-based security to manage the ability to view and work with tickets and configuration items. When organization-based security is enabled, you can view the tickets and CIs that are related to the organization you belong to. You can also view tickets that are related to support groups that you are a member of.