# IT Service Center User Guide

Version 1.20.0

November 15, 2021

*The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.*

*Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.*

*Please visit https://docs.tanium.com for the most current Tanium product documentation.*

*This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.*

*Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.*

*Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.*

*As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.*

*Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, email Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.*

# Table of contents

# About this documentation

This document is for Version 1.20.0.

To download the IT Service Center Administration and User Guides, see IT Service Center Documentation.

# IT Service Center overview

With IT Service Center, you can streamline IT support operations by consolidating IT ticketing and tasks into a single location.

| |
|---|
| Available in: Lightning Experience |
| Available in: **Enterprise** and **Unlimited** editions |
| IT Service Center is available as an add-on license. |

## Manage cases and take action

IT Agents can resolve support tickets more quickly by deploying common actions without leaving IT Service Center. These actions include:

- Reviewing performance events
- Terminating processes
- Starting or stopping system services
- Restarting the computer
- Installing, updating, or removing software

For example, if a user opens a support ticket that requires a software update, the IT Agent can deploy the update to the user's asset with a few clicks directly from IT Service Center. IT Agents can also create a deployment that pushes the same software update to other assets, reducing the possibility of duplicate tickets being opened by other users for the same issue.

## Manage real-time asset data in CMDB

Use the Configuration Management Database (CMDB) integration from Tanium with IT Service Center to manage and store real-time configuration items or components related to IT services. Configuration Items (CI) are components that must be managed to deliver an IT service. By defining a central source of truth for CIs, IT agents and configuration managers can improve service management, reduce time spent on change management, and improve auditing, security and compliance.

### Configuration items

A configuration item is associated with an asset, is governed by IT, and is used for an IT service.

A configuration item can be a Tanium Managed CI or a Tanium Custom CI. Tanium Managed CIs are an asset that has the Tanium Client installed. The information about Tanium Managed CIs comes from the CMDB service in Tanium. You can create Tanium Custom CIs in Salesforce for additional CIs that were not found in Tanium, and these are synchronized with the CMDB on a regular basis.

### Configuration item classes

A configuration item class is a predefined categorization for a configuration item that comes from Tanium, for example, an application, business process, or endpoint.

## Tanium as a Service

The ability to take actions on end user computers is enabled by a connection from IT Service Center with Tanium as a Service (TaaS).

The Tanium platform provides visibility and control of your endpoints. In Tanium, an endpoint is any computer or server on which you can install and run the Tanium Client service. In response to your standard or ad-hoc queries, Tanium can discover and report, within seconds, both static and dynamic real-time data pertaining to the endpoint. In addition to getting data about your endpoints, you can deploy actions to manage and secure your environment.

The operations in the IT Service Center are run by API calls to TaaS, which includes the Tanium™ Discover, Tanium™ Deploy, Tanium™ Map, Tanium™ Interact, and Tanium™ Performance modules. Selected data about Tanium endpoints is stored in Salesforce as Asset objects. To see information about Tanium-managed endpoints in Salesforce, you can view them as Assets.

MORE INFORMATION

- Tanium Discover User Guide
- Tanium Deploy User Guide
- Tanium Map User Guide
- Tanium Interact User Guide
- Tanium Performance User Guide

## Work.com overview

IT Service Center is part of the Work.com suite of solutions. Work.com is the complete employee experience platform for the work-from-anywhere world. Work.com is built on top of the Salesforce Platform and enables employees to be successful from anywhere they work.

When you purchase IT Service Center, you also get Employee Workspace and Employee Concierge. These products enable employees to open cases that get sent to IT Agents in IT Service Center.

### About Employee Workspace

With Employee Workspace, you can give your employees an integrated experience and enable employee productivity and collaboration. Employee Workspace provides a central hub for tools and resources your employees need to work from anywhere.

MORE INFORMATION

Work.com Docs: Employee Workspace

### About Employee Concierge

Employee Concierge is an extension to Employee Workspace that includes a searchable knowledge base and ticketing system, so employees can find solutions and get support when they need it.

MORE INFORMATION

Work.com Docs: Employee Concierge

## Supported languages

The IT Service Center user interface is translated into the following languages:

- Chinese - Simplified: `zh_CN`
- Chinese - Traditional: `zh_TW`
- Dutch: `nl`
- French: `fr`
- German: `de`
- Italian: `it`
- Japanese: `ja`
- Korean: `ko`
- Portuguese (Brazil): `pt_BR`
- Spanish: `es`

# Gaining organizational effectiveness

The four key organizational governance steps to maximizing the value that is delivered by IT Service Center are as follows:

- Align strategic planning to business goals. See Strategic planning on page 11.
- Define distinct roles and responsibilities. See RACI chart on page 11.
- Track operational maturity. See Operational metrics on page 14.
- Validate cross-functional alignment. See Organizational alignment on page 13.

## Strategic planning

Develop a strategic roadmap to align IT Service Center as the single source of truth at the center of all IT Service Management (ITSM) and employee experience activities in your organization. These activities should be aligned to business goals, with buy-in from key stakeholders. These activities include, but are not limited, to:

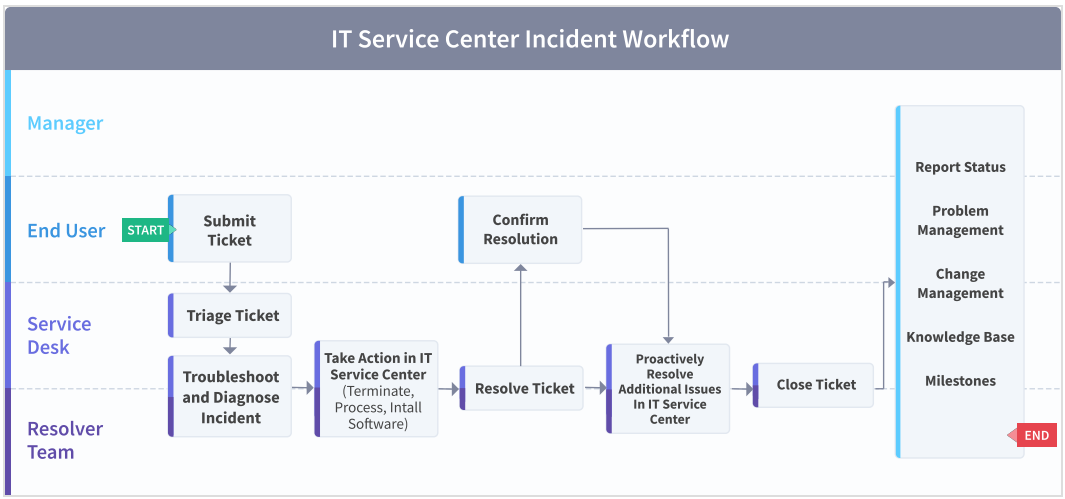
- Update service-level agreements (SLAs) and align activities to key resources for ITSM activities (known in IT Service Center as Milestones) across Service Desk and all resolver teams.
- Align on key incident management workflows both inside and outside the Service Desk.
- Identify key personnel who will need access and training, as well as an ongoing mechanism to train any new joiners.
- Provide and periodically re-evaluate the structure of your IT Service Center program to determine whether it is meeting organizational goals and any opportunities for improvement. Process and governance gaps can cause cascading problems.
- Determine reporting requirements, including segmentation of different reports and bits of information to various resolver teams, leaders, and stakeholders.

## RACI chart

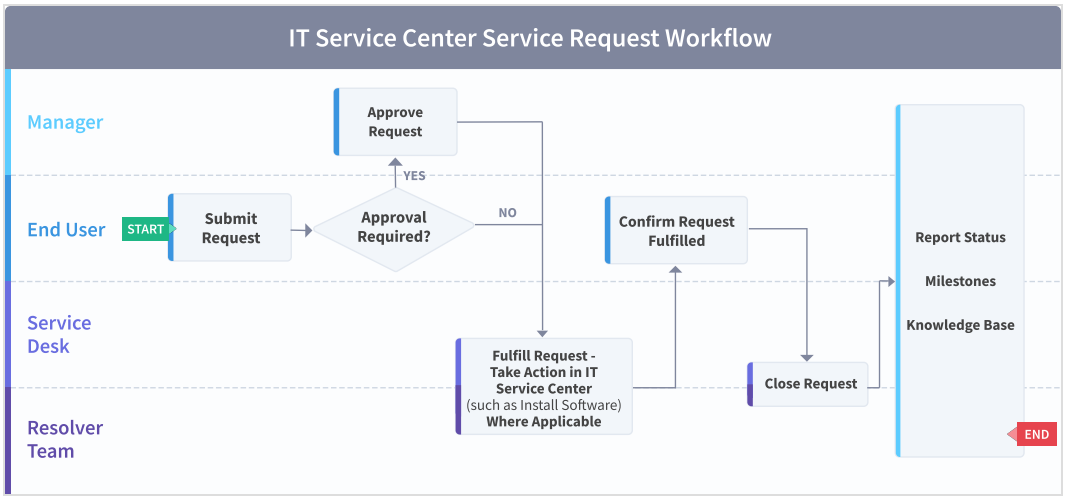
A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across Service Desk and resolver teams in the ITSM program through IT Service Center. Every organization has specific business processes and IT organization demands. The following table represents the IT Service Center point of view for how organizations should align functional resources against Incident Management and Service Request Fulfillment. Use the following table as a baseline example.

| Task | Service Desk | Service Desk Management | Resolver Team | User | Rationale |
|---|---|---|---|---|---|
| Incident logging and categorization | R | - | A | I | The Service Desk is often the intake for a ticket, but the team that resolves the ticket ensures proper categorization. (In some instances, the Service Desk might be the resolver of the ticket.) |
| Incident assignment | R | I | A | - | The team responsible for troubleshooting and resolving the ticket owns incident management. |
| Incident investigation and diagnosis | A | I | R | C | The Service Desk performs an initial analysis of incoming tickets, which also helps IT Service Center learn patterns. |
| Incident resolution and recovery | I | - | A | C/I | The identified resolver team owns the restoration of service when an incident occurs. |
| Incident review and closure | R | I | A | C/I | After a ticket is marked as resolved, the user can confirm the resolution before the ticket is closed. Final closure of the ticket is automatic, and owned by the resolver team. |
| SLA monitoring | R | A | R | - | Service Desk management is responsible for confirming adherence to milestones (SLAs), and determining what changes are needed. |
| Compliance handling | - | R | A/I | C/I | Resolver teams must add enough information in a ticket to stand up to the scrutiny of an audit, with management providing oversight. |

### Incident workflow




**Request workflow**




## Organizational alignment

Successful organizations use IT Service Center across functional silos as a common platform for ITSM and employee engagement, with actions powered by Tanium. Tanium provides a common data schema that enables security, operations, and risk / compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform. This can also serve to take actions through the Tanium platform to mitigate known issues on additional endpoints, enhancing user experience and preventing future tickets.

If the organization isn't aligned and committed to running ITSM, employee experience, and additional actions through IT Service Center, competing data sets and a lack of a holistic view across the entire enterprise of issue resolutions and operational effectiveness will exist.

# Operational metrics

## IT Service Center incident management and service request fulfillment maturity

Managing an ITSM program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your IT Service Center program are as follows:

| Process | Description |
|---|---|
| Usage | how and when IT Service Center for ITSM and employee experience in your organization (for example, whether it is the single tool of record or one of many disparate tools) |
| Automation | how automated IT Service Center is, within your organization, including automatic ticket resolution and automated actions from tickets |
| Functional Integration | how integrated IT Service Center is with the resolver groups within IT, such as Operations, Security, and Service Desk, as well as integrations with external tools such as a Configuration Management Database (CMDB) |
| Reporting | how automated ITSC KPI reporting is, and how tailored that reporting is to different audiences and stakeholders |

## Benchmark metrics

In addition to the key IT Service Center Incident Management and Service Request Fulfillment processes, the two key benchmark metrics that align to the operational maturity of the IT Service Center program to achieve maximum value and success are as follows.

| Executive Metrics | Mean Time to Resolve (MTTR) | SLA Compliance Rate | Tickets Automatically Resolved | Actions Taken From Tickets |
|---|---|---|---|---|
| Description | Average time it takes to resolve an open ticket. This metric can be segmented by additional inputs such as incident severity, resolver team, or specific person. | Percentage of closed tickets that fall within published service level agreements (SLAs). | Number of tickets created through an action in IT Service Center to proactively resolve issues with one or more endpoints. These tickets are created and automatically resolved to maintain record keeping for audit and Change Management purposes. | Number of individual actions all agents performed through the IT Service Center console. This metric can be segmented by additional data such as team and type of action. |
| Instrumentation | Instrumentation (Total Time Spent on Tickets)/ (Number of Tickets In A Certain Time Period) | Boolean/Percentage: (Met SLA = Yes)/Total Number of Tickets | Count Number of tickets with time to resolve = 0 in a given time frame | Count Number of actions taken within a ticket, separated by type, in a given time frame |

| Executive Metrics | Mean Time to Resolve (MTTR) | SLA Compliance Rate | Tickets Automatically Resolved | Actions Taken From Tickets |
|---|---|---|---|---|
| Why this metric matters | Measuring the actual time taken to resolve a ticket, on average, is a key indicator of ITSM effectiveness and user satisfaction. | Determining whether agreed-upon performance benchmarks are being met. | An action taken from IT Service Center, such as software distribution, generates a ticket that is automatically resolved. Each of these tickets is an incident that was prevented, reducing MTTR and increasing organizational effectiveness. | The ability to take actions from tickets is a key differentiator of IT Service Center. Customers who train their support staff to take action from tickets reduce MTTR, improve user satisfaction, and prevent future incidents. |

Use the following table to determine the maturity level for IT Service Center in your organization.

| | | Level 1 (Needs improvement) | Level 2 (Below average) | Level 3 (Average) | Level 4 (Above average) | Level 5 (Optimized) |
|---|---|---|---|---|---|---|
| Process | Usage | Multiple competing ITSM tools used with no clear delineation or consistent usage. All remediations are reactive. | Frameworks applied with inconsistent processes. No more than two ITSM tools used across the estate. | Frameworks applied with repeatable processes. Single ITSM tool serves as a system of record. | Frameworks applied with regular reviews for efficacy. Single ITSM tool is used. Processes optimized and automated where possible. Proactive support complements reactive support. | Customer-centric, agile service delivery through a single ITSM tool and repeatable, automated processes that are regularly measured and optimized through KPI reporting. |

| | | Level 1 (Needs improvement) | Level 2 (Below average) | Level 3 (Average) | Level 4 (Above average) | Level 5 (Optimized) |
|---|---|---|---|---|---|---|
| | Automation | No automation; all ticket resolution is manual. | Understand and prioritize actions that can be taken from tickets. Defined KPI reporting for automation. | Automatic ticket resolution available and guard-railed with appropriate RBAC | Automatic ticket creation and closing are built into processes for certain tickets, tracked with Change Control as Standard changes | Automatic ticket creation and closing are built into processes for certain tickets, tracked with Change Control as Standard changes. Ticket routing is done more automatically based on workflows. |
| | Functional integration | N/A | Internal reporting leveraged to get baseline metrics for KPIs | KPI reports created. Relevant support people trained to deliver ticket automations through IT Service Center | KPI reports are automatically generated and configured to send to stakeholders at identified intervals. Integrated with other key tools in the organization | Real-time monitoring to alert of a potentially problematic service (ticket spike) |
| | Reporting | Reporting is only ad-hoc and not actively measuring identified KPIs | KPIs identified and irregularly tracked to identify gaps in service delivery | Automated: KPI reports for Service Desk only | Automated: KPI reports sent to key stakeholders from CIO/Head of IT, to resolver groups, and to Service Desk | Automated: Tailored and specialized KPI reports sent to key stakeholders from CIO/Head of IT, to resolver groups, and to Service Desk |

| | | Level 1 (Needs improvement) | Level 2 (Below average) | Level 3 (Average) | Level 4 (Above average) | Level 5 (Optimized) |
|---|---|---|---|---|---|---|
| Metrics | Mean Time to Resolve (MTTR) | Not measured | Measured in aggregate | Measured by team | Measured by team and severity | Measured by team, severity, and ticket type |
| | SLA Compliance Rate | Not measured - No SLAs | Not measured - SLOs (Service Level Objectives) in place | > 50% | < 75% | > 95%<br>SLAs measured by incident severity and optimized |
| | Tickets Automatically Resolved | 0-5% | 5-10% | 10-15% | 15-20% | 20-25% |
| | Actions Taken from Tickets | 0 - Not set up | 0 - Not set up | Certain actions, limited to Service Desk | All resolver groups have access, not all available actions are approved | All available actions approved and taken |

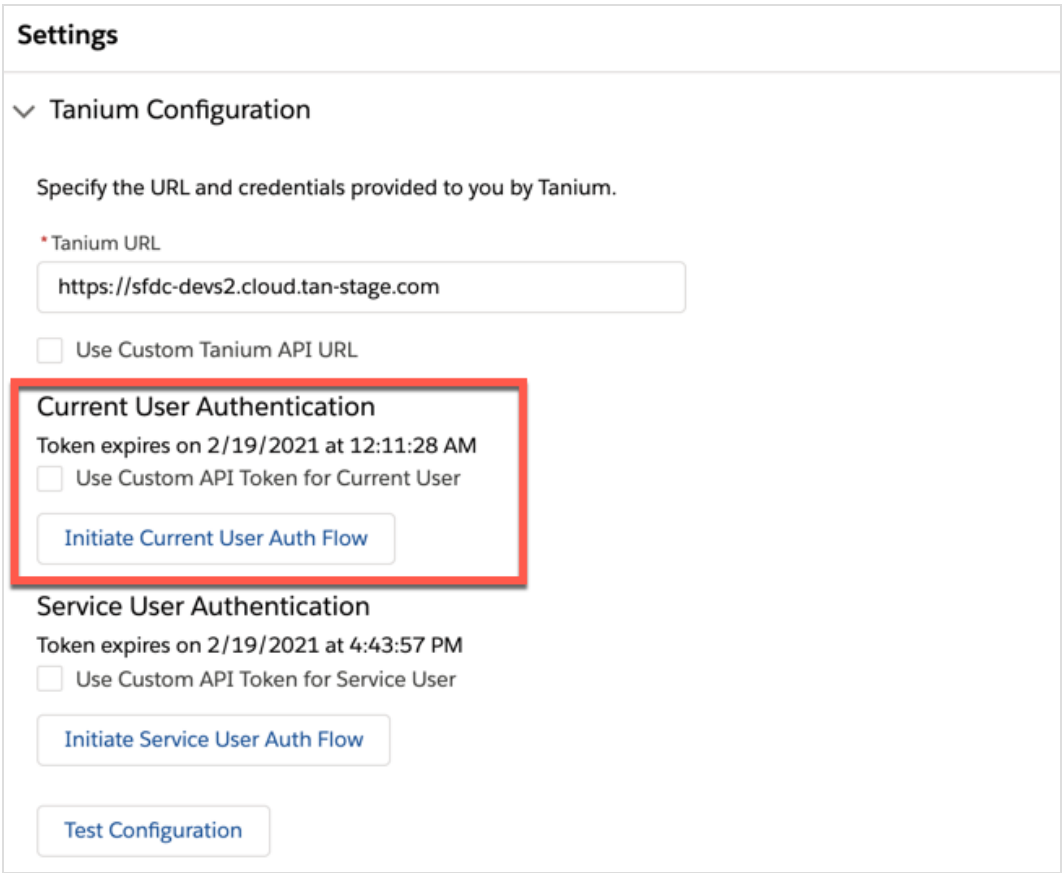
# Authenticate with Tanium as a Service

Authenticate your Salesforce user ID with Tanium as a Service (TaaS) to have permission to view and operate on assets in IT Service Center.

IMPORTANT

If you do not log in for 30 or more days, you must repeat these steps.

1. To open IT Service Center, log into your Salesforce org and use the App Launcher to search for and select **IT Service Center**.
2. From the IT Service Center menu, go to **Settings > Tanium**.
3. Click **Initiate Current User Auth Flow**.
4. In the page that pops up, click **Authorize**.
5. The expiration date under **Current User Authorization** is updated.



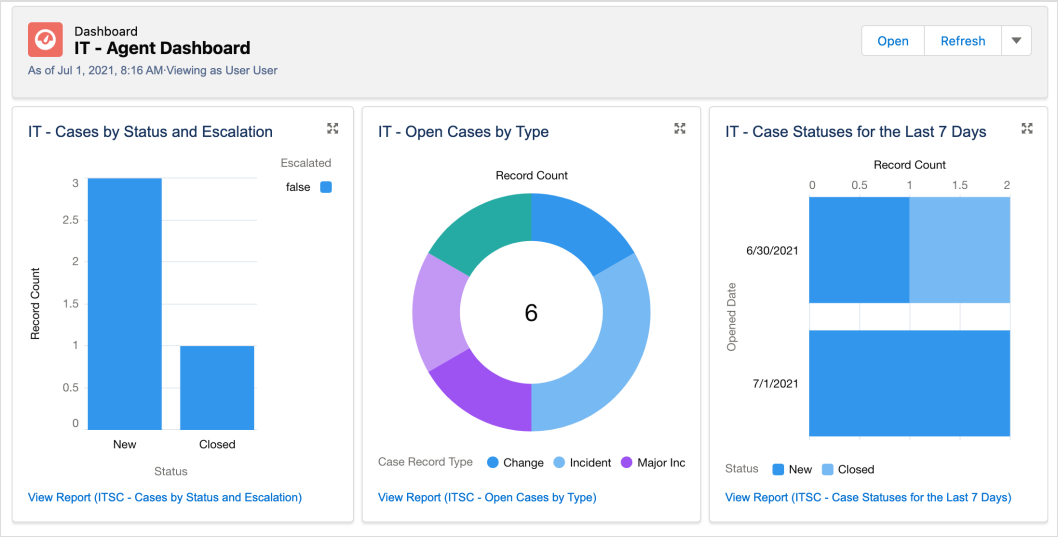
# Manage IT cases

After employees create tickets in the Employee Concierge, an IT agent can manage the cases from IT Service Center. The IT Agent dashboard provides interactive reports with trends and insights about your internal IT cases. You can view IT cases by status, type, opened date, and so on.

As an IT agent, you can manage IT tickets, view information about end user computers, and manage end user computers by deploying software or performance actions.

## View IT Agent dashboard

View the IT Agent Dashboard on the home page when you open IT Service Center. The dashboard gives a summary of all cases that are open.




## View cases

To view cases in more detail, go to the IT Service Center menu and click **Cases**. Click the menu  for the Cases page to switch to different views of the cases, such as **My Open Cases**, **All Open Cases**, **Open Incident Cases**, and so on.

## Incident

An incident is a case that is related to an issue that a user is experiencing, such as a disruption of operations, services, or functions.

End user employees can use Employee Concierge to create a ticket for issues they are experiencing, such as trouble with software on their personal computer, that results in an incident case record type.

After the ticket gets created, the IT agent can use IT Service Center to resolve the ticket by viewing information about the associated asset, and taking actions on the associated computer such as terminating a process or deploying software.

ABOUT INCIDENT CASES

**Created by user type:** Employee

**Phases:** New > In Progress > Pending > Transferred > Resolved > Closed

**Default Case Templates:** Force Terminate Process, Restart Endpoint, Restart Service, Start Service, Stop Service, Terminate Process


If you create an incident on behalf of an end user, you must resolve and close the ticket. The end user can only resolve and close tickets that they opened.

1. From the IT Service Center home page, click the **Cases** tab. Click **New**.
2. Choose the **Incident** case record type.
3. Click **Save**.

# Major Incident

Log a ticket for a major loss or disruption of operations, services, or functions.

## About major incident cases

**Created by user type:** Administrator, IT Agent

**Phases:** New > In Progress > Resolved > Review & Postmortem > Closed

## Create a major incident

1. From the IT Service Center home page, click the **Cases** tab. Click **New**.
2. Choose the **Major Incident** case record type.
3. Fill out information associated with the case.
4. Click **Save**.

## View major incident timings

Major incident timings provide details on how long it takes a major incident to be put into progress, mitigated, and completed. The times provided are based on the local time of the user that is signed in to IT Service Center.

1. In a major incident case, expand the **Scope Details** section.
2. In the **Total Duration** tile, click **View All**. The following times are displayed:

   **Reported Time**

   The time that the customer opened the major incident.

**Start Time**

The time that the agent first looked at the major incident in IT Service Center.

**Team Notified Time**

The time that the team was notified about the case, either by entering a state as defined by the **Team Notified** setting, or by a major incident action.

**Mitigated Time**

The time that the case has entered a mitigated state, as defined by the **Case Mitigated** setting. For more information, see the *IT Service Center Administration Guide*.

**End Time**

The time that the case has entered an end state, as defined by the **Case Ended** setting. For more information, see the *IT Service Center Administration Guide*.

**Team Engaged Time**

When a major incident enters one of the selected states, the case is no longer on hold, and cumulative on hold time for the case stops. From this time on, time is added to the **Total Duration** field. . For more information, see the *IT Service Center Administration Guide*.

### Run major incident actions

Major incident actions are flows that can be configured by the ITSC administrator. For more information, see the *IT Service Center Administration Guide*.

By default, the **ITSC - Major Incident Team Notification** flow is included with IT Service Center, which is a flow that sends a notification to a set of users.

1. In a major incident case, go to the **Actions & Recommendations** section.
2. Click the name of the flow that you want to start running. For example, click **ITSC - Major Incident Team Notification**, the **Continue** to run the flow.
3. To view a list of flows that have run for the major incident, click the **History** tab in the **Actions & Recommendations** section.

## Problem

You might create a problem ticket if you have an incident that is a part of a larger problem that needs to be investigated.A problem is a case that affects something broader than a single user, such as a systemic problem that occurs over time and must be investigated for root cause analysis.

For example, many users are reporting recurring system latency issues, but the root cause of why these issues keep returning is undetermined. You can associate all of the incidents that these users created into a problem, and continue to analyze the cases as a group.

ABOUT PROBLEM CASES

**Created by user type:** IT Agent

**Phases:** New > Analyzed > Workaround Documented > Known Error > Change Created > Resolved > Closed

1. From the IT Service Center home page, click the **Cases** tab. Click **New**.
2. Choose the **Problem** case record type. Click **Save**.

## Create known error or service knowledge

You can create a known error or service knowledge to document a problem in a knowledge article. After you create a known error article, the article is attached to any cases that are associated with the problem. This article remains in draft state and is not visible to other users until it gets published.


To enable all users to see the known errors, ask your administrator to configure publishing workflows. For more information see *Create publishing workflows for known errors and service knowledge* in the IT Service Center Administration Guide.

1. In the problem case, click **Create Known Error** or **Create Service Knowledge**.
2. Enter a title, URL, details, and workaround. Click **Save**.
3. To make the knowledge article visible to other users, you must publish the article. To publish a knowledge article, see Service Cloud Help: Publish Articles and Translations.
4. You can see the cases that are related to a knowledge article when you edit the article in Salesforce Knowledge.

## Conduct root cause analysis

By default, you can document the root cause in a text field in the problem case. Your administrator can update the configuration to add a Root Causes related list to the **ITSC - Problem Record** page.

1. In the case, open the **Root Causes** related list. Click **New**.
2. Add details about the root cause analysis that you are conducting, including the primary cause, dates, and analysis information. Save your changes.
3. You can view a list of all the root causes that were added to the problem in the related list.

For more information about configuring multiple root causes to be attached to the problem case, see the *IT Service Center Administration Guide*.

## Automatically generate problem cases

For incidents, the ITSC administrator can enable a setting that automatically generates and associates a problem case after a certain number of incident cases are associated with an incident case. If this incident case already has a problem, major incident, or change case associated, the problem is not generated.

For more information about the **Automatically Generate Problem Cases** setting, see the *IT Service Center Administration Guide*.

# Change

Track changes that need to be made to an organization. These changes typically need to go through a discussion and approval process by a change approval board (CAB) before they get implemented.

A change case is for when an existing system requires approvals before being updated. There might be approval rules and workflows required to move to a resolution.

USER PERMISSIONS

| User Permissions Needed | |
|---|---|
| To create a change case: | IT Service Center App User, Change Calendar Basic Access permission sets |
| To add events to the change calendar: | Change Calendar Admin Access permission set |
| To create custom change management rules: | Change Calendar Admin Access permission set |

## About change cases

**Created by user type:** Administrator, IT Agent

**Phases:** New > Request for Change > Submitted for Approval > Approved > Rejected > Resolved > Closed

## Create change case

1. From the IT Service Center home page, click the **Cases** tab. Click **New**.
2. Choose the **Change** case record type and fill out the required fields.
3. Click **Save**. After the change is created with planned dates, it gets added to the change calendar.

RESOLVE SCHEDULING CONFLICTS

You might get a scheduling conflict if an event already exists on the change calendar during the planned start or end time, or if a change management rule is in place that requires changes to be scheduled at a specific time. Click **View Change Calendar** and resolve the timing of your change case and save your updates. For more information about the change calendar and rules, see Manage change calendar on page 24 and Configure change management rules on page 25.

ASSESS RISK

After you save a change case, the risk level is determined based on the change management risk score settings. Change managers can determine the fields that contribute to the risk score. For more information, see *Customize risk scores* in the IT Service Center Administration Guide.

## Manage change calendar

You can use the change calendar to configure and visualize the planned change events.

VIEW CHANGE CALENDAR

- To view the change calendar, go to the IT Service Center menu and click **Change Calendar**.
- To customize the event types that are included in the calendar view, select the event types you want to include.

The following event types are included by default:

- Freeze: A scheduled time frame during which changes cannot occur.
- Change: An update attached to a Change case.
- Change window: An allowed time frame for changes to occur.
- Outage: A scheduled time that a system is not available.

ADD EVENTS TO THE CHANGE CALENDAR

If you have the Change Calendar Admin Access permission set, you can add events to the change calendar.

1. Go to the IT Service Center menu and click **Change Calendar**.
2. Click **New Event**, **New Freeze**, or **New Change Window**, depending on which type event you want to create.
3. Enter date and time information for the event and click **Save**.

### Configure change management rules

The change manager can create rules for the following scenarios:

- Change Window Rule - When enabled, changes must occur during a defined change window.
- Field Match Overlap Rule - For a defined field, allow a maximum number of matches for a value on other change cases. For example, you might allow a maximum of 3 changes to be scheduled on the Category field with Hardware selected.
- Freeze Rule - When enabled, changes cannot be scheduled during a freeze period.
- Overlap Rule - When enabled, any overlaps with other changes are returned when you save the change case.

With the rule, you can choose to warn or return an error and prevent the change case from being created.

1. Go to the IT Service Center menu and click **Change Management Rules**.
2. Click **New** and choose the type of rule that you want to create.
3. Fill out the required fields for the rule. To activate the rule when you save, select **Is Active**.
4. Save your changes. The conditions defined in the rule are immediately in effect for any new change cases that get created. If you need to deactivate a rule, you can edit the rule to deselect **Is Active**.

## Request

A request is a service request from a user for access, advice, information, a standard change, or documentation. The request is not related to a failure in the IT infrastructure.

### About request cases

**Created by user type:** Employee

**Default Case Templates:** Install Software, Remove Software, Update Software

### Create a request

1. From the IT Service Center home page, click the **Cases** tab. Click **New**.
2. Choose the **Request** case record type.
3. Click **Save**.

## Update cases

Change the owner, record type, or escalate the case.

### Change case owner

1. Open a case, or select one or more cases from a list view. Click **Change Owner**.
2. Search for the person to which you want to assign the case.
3. To send the new owner a notification, select **Send Notification Email**. Click **Submit**.

### Change record type

If the case got created with the wrong record type (for example, a user created an incident that is actually a request), you can update it to the correct type.

1. To update the owner of a case, click  , then **Change Record Type**.
2. Select the new record type and click **Next**.
3. Edit the case. Depending on the type of case that you selected, you might need to update the required fields.

### Escalate case

Assign the case to a different user or queue.

1. Within the case, click the **Activity > Escalation** tab.
2. Select **Escalated** and provide an **Escalation Reason**.
3. Set the **Case Owner**.
4. Click **Save**. When the case is escalated, it is in **Transferred** status.

### Attach files

1. From your case, go to the **Attachments** tab.
2. To add files, click **Upload Files** and select documents from your computer.

## Track activity

Track activity for a case to see any changes to the case, comments, or actions that have been taken to resolve the case.

### View case activity

Within a case, you can view a feed of the updates that have been made in the **Activity** tab.

### Comment on a case

You can collaborate on the case by adding chatter comments in the **Post** area on the **Activity** tab. For more information about posting and chatter, see Salesforce Help: Posting Overview and Salesforce Help: @Mention People and Groups in Posts and Comments.

### Follow case updates

Click **+ Follow** in the case to get emails when the case gets updated.

## Track related work

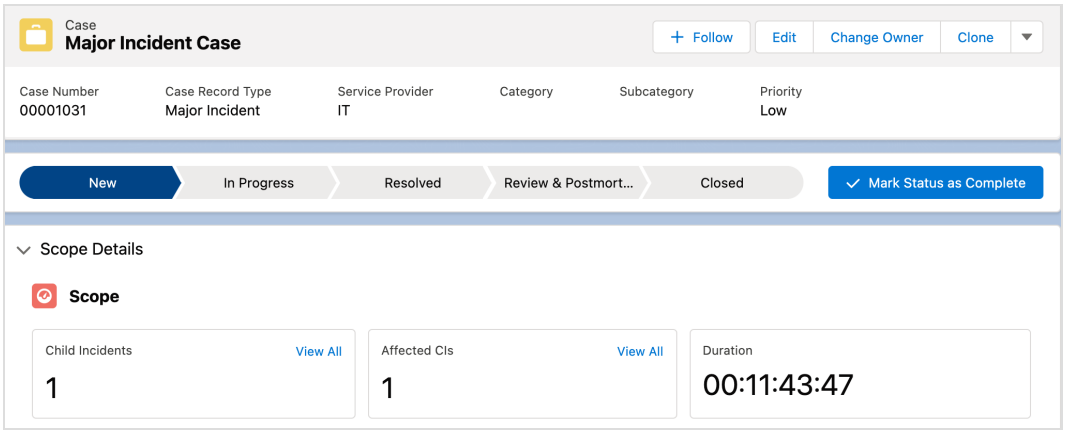
Use associations to generate a list of incidents, major incidents, problems, requests, changes, or configuration items that are associated with a case.

Cases can be related to each other by associations. Many different incidents might be related to other incidents, a single problem, and so on.

Cases to other cases and cases to configuration items are both many-to-many relationships.

### Expand scope details

In the **Scope Details** section of incidents and major incidents, you can view the child incidents, affected configuration items (CIs), and duration for the case. You can click the links to view the details.




**Affected CIs** include configuration items that are directly related to the case.

### Add a task

You can add tasks to track individual work items associated with the case.

1. In the case, click **Attachments**.In the **Open Activities** section, click **New Task**.
2. Add details about the task, including the description, status, assignee, and priority. Save your changes.
3. Any open tasks related to a case are displayed in the **Open Activities** section. When you complete a task, it is moved to the **Activity History** section.

### Add associations

From the **Associations** tab, click **Add** in the category for which you want to add an association.

For incidents, the ITSC administrator can enable a setting that automatically generates and associates a problem case after a certain number of incident cases are associated with an incident case. If this incident case already has a problem, major incident, or change case associated, the problem is not generated.

For more information about the **Automatically Generate Problem Cases** setting, see the *IT Service Center Administration Guide*.

### Remove associations

Click down arrow next to the associated case, problem, request, change or asset, and select **Remove**.

## View service and remediation insights

You can use these insights to associate similar cases, or identify possible resolutions and remediation actions.

### View service insights

Use service insights to identify similar open cases in IT Service Center. Service insights compare description and subject fields of other open incidents, problems, and changes.

1. Open an incident, major incident, or problem case.
2. Go to the **Service Insights** tab. You might need to click **More** to see the tab.
3. Expand the sections to view related incidents, problems, and changes.
4. If a listed case is related, you can create an association to track the cases together.

### View remediation insights

Use remediation insights to review resolutions for similar cases that have already been resolved or closed.

1. Open an incident, major incident, or problem case.
2. Go to the **Remediation Insights** tab. You might need to click **More** to see the tab.
3. Expand the sections to view related incidents, problems, and changes.

## Resolve a case

When the work for a case is complete, resolve the case.


If you create an incident on behalf of an end user, you must resolve and close the ticket. The end user can only resolve and close tickets that they opened.

1. Within the case, go to the **Resolution Information** section.
2. Choose a **Resolution Type** and provide details about the resolution and save your changes.
3. In the status bar for the case, click **Resolved**, then click **Mark as Current Status**.

Cases that are in **Resolved** state are automatically moved to **Closed** state after seven days. You cannot edit or reopen a closed case.

### Close a case and all related cases

1. Change the case to Closed status. In the status section, click **Closed** and then **Set as Current Status**.
2. If the case has associated records, you can review a list and choose to close the cases. Select **Close Record(s)** and click **OK**.

# Manage configuration items

View details about the computer that is associated with a case.

When an end user opens a ticket, their user name is saved as a part of the ticket and their associated computer information gets retrieved. Then, as an IT agent, you can then get information about and take actions on the user's computer directly from the IT Service Center user interface.

The data that you view about the end user's computer in the IT Service Center is live from the configuration management database (CMDB) in Tanium. This capability is enabled by the Tanium Client software running on each endpoint. These clients return information to Tanium as a Service (TaaS), including computer name and hardware information, current health, software, and performance statistics. This information is stored as an asset in IT Service Center. If the end user turns off their computer, you can see the information about the asset in its last known state.

IMPORTANT If you edit the details of an asset in the IT Service Center, the edits that you make will likely be replaced with new data from Tanium the next time the data gets refreshed. Similarly, if you delete an asset but it still exists in Tanium, the asset item will get re-created with the next data import.

## View Primary CI details from a case

Drill into details about the associated computer that is attached to the case.

1. From the IT Service Center menu, go to **Cases** and click a case.
2. Expand the **Primary CI Details**. Review the information about the CI.
3. If the CI is a Tanium Managed CI, you can pull the latest status from Tanium. Click Refresh next to the **Data Last Updated** field.

## View configuration items

1. To view a list of all assets, go to the IT Service Center menu and select **Assets**.
2. By default, the list displays a list of recently viewed assets. To display a list of all assets, click and select **All Configuration Items**.
3. Click the name of an asset to view details. Click the **More > Associations** tab to view all cases that are associated with the configuration item.

## View CI relationships

For Tanium Managed CIs, connected endpoints and services are automatically identified and added as relationships in the CI. You can use these relationships to help identify dependencies and understand impact of changes to a specific CI. For example, you might have a server that needs maintenance. You can use the CI relationships to identify any connected services or servers that are

affected.

1. From the IT Service Center menu, click **Assets**.
2. Open a configuration item. Click the **CI Relationships** tab. You can view dependent application services, incoming and outgoing connections, and peers.

# Manage performance

View the health of an asset, including the processes and services that are running on the asset. Force terminate processes, start or stop system services, or restart the computer entirely.


You can directly connect only to an endpoint that has an IPv4 address.

## Review health events

In a case, click **Primary CI Details**, then the **Health Events** tab to review the performance events that have occurred for the asset.

The following table summarizes the types of events and default conditions that trigger the events from Tanium. If you want to customize these event triggers, configure profiles in the Tanium Performance module in your Tanium as a Service instance. See Tanium Performance User Guide: Configuring profiles.

| Event Type | Associated Rules |
|---|---|
| CPU | Any of the following conditions trigger an event:<br>• (Windows, Mac, Linux) CPU utilization > 90% AND Kernel Time > 40%<br>• (Windows) DPC time > 20%<br>• (Mac, Linux) Load average [15m] > CPU core count x 0.9 |
| Available Memory | (All OS - for at least 10 minutes)<br>• Available memory < 250 MB<br>• Available memory < 10% |
| Disk Capacity | (All OS)<br>• Disk capacity < 500 MB<br>• Disk capacity < 10% |
| Disk Latency | (All OS - for at least 10 minutes)<br>• Read latency < 250 ms<br>• Write latency < 10% |
| Application Crashes | (Windows) Any application crash occurs |
| System Crashes | (Windows) System crash occurs |

## Restart operating system

If an operating system restart is required to resolve the case, you can initiate the restart from IT Service Center.

1. In the case, click the **Primary CI Details** tab, then **Activity**.
2. To restart the computer's operating system, click **Restart Asset**.

## Terminate processes

If a process is using too much CPU or memory, you might consider terminating the process to resolve performance issues.



To test the functionality of stopping a process, start a test process on the endpoint.

1. In the case, click the **Primary CI Details** tab, then **Activity**. Review the list of active processes.
2. Sort the active process list by clicking the **CPU** or **Memory** column.
3. Stop individual processes. To ask the process or service to stop, click  in the row and select **Terminate Process**. To force the process to stop, select **Force Terminate Process**.

## Manage system services

You can start, stop, or restart system services to resolve problems.

1. In the case, click the **Primary CI Details** tab, then **Activity**. Review the list of system services.
2. Stop, restart, or start services. Click  in the row and select the action on the service that you want to take.

# Deploy software

You can check the software that exists on the computer - is it out of date, does it need to be updated or removed? With a few clicks, you can deploy actions that install, update, or uninstall software.

## Manage out of date software

Check the asset for any software that needs to be updated, and deploy software updates.

1. Within the case, click the **Primary CI Details** tab, then **Software**.
2. Click **Manage Out of Date Software** and review the list of available software updates. Select the update titles that you want to install. Click **Next**.
3. Choose whether you want to restart the endpoint after running the update, and click **Deploy**.
4. Click the **Feed** tab in the case to review the list of activities for the deployment.

## Install new software

Install new software on the asset.

1. Within the case, click **Primary CI Details**, then **Software**.
2. Click **Install New Software** and review the list of available software from the Tanium application catalog. Select the software titles that you want to install. Click **Next**.
3. Choose whether you want to restart the endpoint after running the update, and click **Deploy**.
4. Click the **Feed** tab in the case to review the list of activities for the deployment.

## Remove software

Uninstall software from the asset.

1. Within the case, click the **Primary CI Details** tab, then **Software**.
2. Click **Remove Software** and review the list of available software that can be removed from the endpoint. Select the software titles that you want to remove. Click **Next**.
3. Choose whether you want to restart the endpoint after running the update, and click **Deploy**.
4. Click the **Feed** tab in the case to review the list of activities for the deployment.

# Automate IT Service Center with flows

Use flows to automate specific IT tasks such as deploying packages or software, based on a set of conditions.

## Default flows

The following flows are included by default with IT Service Center. To edit the flows from Setup, enter `flow` in the Quick Find box, and then select **Flows**.

**ITSC - Auto Close Cases**

A triggered action at 12:00 AM closes all incidents and requests that were resolved in the past seven days.

**ITSC - Case Notifications**

A triggered action when a status changes on a problem case that sends an email to notify users on associated incident cases.

**ITSC - Case Owner Changed**

A triggered action when an incident or request case record is saved. If the owner for the case has changed, the action sets the status of the case to **Transferred**.

**ITSC - Change Approval**

A triggered action that runs after a change case record is saved and submitted for approval.

**ITSC - Set Case to Known Error**

A triggered action when a known error is created that changes the status of the problem case to **Known Problem**.

**ITSC - Share Comments**

A triggered action when an incident status is changed to resolved that copies comments from the resolved incident to associated incidents.

**ITSC - Major Incident Team Notification**

A triggered action to send a status notification and set the **Team Notified** date and time.

## Flow actions

You can create flows with the following flow actions when IT Service Center is installed:

**Copy Current Feed to Associated Cases**

Copies chatter feed comments to associated cases.

**Find Primary Assets By User**

Return a list of assets and basic information that list the specified email address as the primary user.

**Deploy Package**

Deploy a Tanium package to an asset. This package typically includes a script and set of files that run on the asset as a Tanium action.

**Manage Software Deployments**

Install, update, or remove software packages on a specified asset.

**Query Asset Information**

Return field values for the selected asset.

**Find Applicable Software**

Determine the software updates that are available for a selected set of assets.

**Send Email to Associated Case Owners**

Send email to owners of associated cases.

## Create an IT Service Center flow

1. From Setup, go to **Process Automation > Flows > New Flow**.
2. Choose the type of trigger that you want to use for your flow. For testing purposes, choose **Autolaunched Flow (No Trigger)**.
3. Drag an Action to your flow. Click **IT Service Center** to view the available actions.

## More information

Automate Your Business Processes: Flows

# Maximize IT Service Center metrics

The following table lists contributing factors into why the metrics might not be meeting your goals, and corrective actions you can make.

## Mean Time to Resolve (MTTR)

Mean time to resolution by case owner is included as a report in IT Service Center. From the IT Service Center menu, click **Reports > ITSC - Mean Time to Resolution**.

| Contributing Factor | Corrective Action(s) |
|---|---|
| Severity not captured | • Capture severity and consider all tickets in aggregate for the most complete picture of the overall success of the program.<br>• Separate MTTR by severity to gain more specific insight into how the ITSM program is performing. |
| No critical incident process | A critical incident affects key sites or infrastructure that have effects across an organization.<br>• Flag critical incidents in IT Service Center and track critical incidents as a separate metric. If you do not track critical incidents as a separate metric, they are counted in the same buckets as other incidents that, while impactful, do not affect the organization to such a degree. |
| Unclear goal alignment | Set clear goals that are understood by all key IT stakeholders will help to establish a shared sense of purpose. Strategic planning is important for the success of an ITSM program because it provides the why behind the how. If an organization wants to manage MTTR, it's important to understand why this is an important goal and how it will benefit the organization. |
| Ownership structure unclear | • Create a RACI chart.<br>• Establish clear communications on which stakeholders are responsible for tracking and reducing MTTR. |

## SLA Compliance Rate

| Contributing Factor | Corrective Action(s) |
|---|---|
| No SLAs | • Set formal Service Level Objectives (SLOs) between IT and business stakeholders.<br>• Measure compliance to SLOs.<br>• Distill SLOs to SLA that can be agreed upon by both IT and business stakeholders. |

| Contributing Factor | Corrective Action(s) |
|---|---|
| SLAs too broad | Broad SLAs can create a skewed picture of the success of the ITSM program.<br>• Set SLAs to consider severity, impact, and type of work being done.<br>• Customize SLAs for individual teams based on process variations and organizational need, for more granular reporting and alignment of goals to employee experience. |
| SLAs not enforced/ enforceable | With no mechanism for determining compliance and remediating non-compliance, SLA Compliance Rate can become a metric with no drive for change or improvement.<br>• Establish periodic SLA reviews with all key stakeholders. Discuss compliance against current requirements and ongoing requirements and goals.<br>• Review, revise, and refine metrics to confirm goals are achievable and reflect the current state of ITSM. |

## Tickets Automatically Resolved

| Contributing Factor | Corrective Action(s) |
|---|---|
| Unclear division of responsibility | • Establish an agreed upon RACI chart and appropriate training to make sure the proper actions are taken by the correct groups. Service Desk and individual resolver teams might be assigned different actions to take on endpoints. See RACI chart on page 11. |
| Risk seen in taking automatic action | • Log changes made to endpoints in incident tickets. |
| Lack of robust Change Management | • Begin working on a change management process to avoid changes being made with no logging. |
| Audit requirements | • Determine audit requirements and build IT Service Center workflows around capturing the appropriate information. |

## Actions Taken From Ticket

| Contributing Factor | Corrective Action(s) |
|---|---|
| Unclear division of responsibility | • Establish an agreed upon RACI chart and appropriate training to make sure the proper actions are taken by the correct groups. Service Desk and individual resolver teams might be assigned different actions to take on endpoints. See RACI chart on page 11. |

| Contributing Factor | Corrective Action(s) |
| --- | --- |
| Concern for adverse impact | • Build confirmation steps into the workflow to confirm the selected action does not cause adverse impact to endpoints.<br>• Use Tanium capabilities to roll back changes that end up having adverse impact. Changes are logged and vetted, minimizing risk and providing a mechnism to roll back if necessary. |
| Lack of robust Change Management | • Log changes made to endpoints in incident tickets.<br>• Begin working on a change management process to avoid changes being made with no logging. |
| No CMDB / Asset Database | • Create tickets that identify endpoints affected and action taken to preserve information in the absence of a CMDB or asset database. |
| Audit requirements | • Determine audit requirements and build IT Service Center workflows around capturing the appropriate information. |