Washington DC Proactive Service Experience Workflows

Last updated: 12/16/2025

servicenow

Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products or services is intended or should be inferred.

Please read the ServiceNow Website Terms of Use at www.servicenow.com/terms-of-use.html

Company Headquarters
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

Table of Contents

Proactive Service Experience Workflows

Deliver end-to-end support, while understanding customer impact, and offering transparent communication to all parties involved in the support process.

The following image shows the main capabilities of Proactive Service Experience Workflows.

Explore Learn about how service providers and customers use Proactive Service Experience Workflows.	Configure Plan and configure your implementation.
Use Using Proactive Service Experience Workflows.	Reference Get details about domain separation for Proactive Service Experience Workflows.

Exploring the Proactive Service Experience Workflows architecture

Learn how you can use the Proactive Service Experience Workflows application to automatically initiate workflows that resolve network-initiated incidents and proactively notify impacted customers.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Proactive Service Experience Workflows capabilities

Proactive Service Experience Workflows deliver end-to-end support, while understanding customer impact, and offering transparent communication to all parties involved in the support process. Telecommunications, Media, and Technology service providers can:

- Identify affected customer accounts based on one or more configuration items associated with upstream services that are tied to an install base.
- With Operations Account 360, use data from ITSM and CSM to drill down into customer accounts and visualize key information about the account.
- Generate proactive cases that include synchronizations of certain fields on case insert, incident resolution, or closure of a change request.
- Reduce administrative setup and overhead with enhanced incident and change request forms in the Service Operations Workspace.
- Resolve minor cases without intervention by customer support agents.
- Provide capabilities for technical support agents to communicate with external customers without navigating between incident or change requests, and associated case records.
- Use five unique Flow Designer flows that can be modified to suit your business needs.
- Escalate incidents for faster action based on a preconfigured decision table.
- Use extended CMDB CI Classes common to SD-Wan edge infrastructure
- Create incident records from certain API clients based on TM Forum TMF621 Rest API standards.
- Use dedicated roles that enable technical support agents to see both ITSM and CSM and applications.

For information about the architectural components of the Proactive Service Experience Workflows application, see Proactive Service Experience Workflows architecture.

You can also add classes to the CMDB CI classes that target the SD WAN edge infrastructure as part of the CMDB CI Class Models application. See CMDB CI classes for Proactive Service Experience Workflows for more details.

Proactive Service Experience Workflows architecture

There are multiple components that make up the architecture of the Proactive Service Experience Workflows application.

The main components are as follows:

- Flows and subflows
- Escalation stages
- Decision tables
- Messages
- Business rule
- Client scripts
- System properties
- Roles
- Assignment groups
- Service Operations Workspace

Flows and subflows

A workflow is triggered when an incident is created with the SD-WAN category and one of these five subcategories:

- Link Failure
- Device Failure
- Protocol Failure
- Soft-WAN Link Failure
- Software Failure

Each category has subflows for each assignment group and a level of escalation for a total of 27 subflows. These subflows are a starting point created primarily for network operations outages, but can be reused and extended for other use cases.

Escalation stages

The five stages of escalation are as follows:

- Triage
- L1 investigation
- L2 investigation
- L3 investigation
- Resolution

Proactive Service Experience Workflows uses these stage values to trigger the appropriate decision in the Incident Escalation Policy [sys_hub_flow] decision table. This table triggers the correct subflow during incident escalation. During each stage of escalation, an incident task is created and maintained for that assignment group. The incident information synchronizes to the incident task from a business rule and includes the following:

- Short description
- Priority
- State
- Work notes that the assigned person in the assignment group adds to the incident
- Message content that is embedded in the incident by the workflow

Decision tables

Based on the defined condition, Flow Designer works with the Incident Escalation Policy [sys_hub_flow] decision table to determine which subflow to generate at certain escalation points.

Messages

Each subflow in Proactive Service Experience Workflows is associated with a message file that provides instructions for agents to use to troubleshoot, escalate, and resolve network-initiated incidents. For more information about how to customize the default instructions for your internal troubleshooting processes, see Customize message files.

Business rules

The `Sync to tsm incident task` business rule determines the information that synchronizes from the incident to the incident task, including:

- Short description
- Priority
- State
- Assignment group
- Assignee
- Work notes that the assigned person in the assignment group adds to the incident

Roles

The `sn_ind_tsm_core.noc_agent` role is available with the Proactive Service Experience Workflows application. This role when added, ensures that the technical support agent can see the relevant information between ITSM and CSM applications. This role includes the following:

- itil
- wm_initiator
- wm_read
- sn_customerservice.case_viewer
- sn_customerservice.customer_data_viewer

Several assignment groups are included with this role and other groups can also have the admin role. The `sn_ind_tsm_sdwan.ticket_integrator` role can be used for trouble tickets created from the TMF 621 Open API use cases.

Assignment groups

Workflows involve network-related personnel, including network coordinators and engineers. All assignment groups have the base `sn_ind_tsm_sdwan.PSEW_USER` system role.

Note:
These assignment groups are a starting point, created primarily for network operation support.

Network coordinator

The network coordinator's tasks and responsibilities are as follows:

- Manage and triage incidents from the network management systems
- Assess the impact and define the incident priority
- Refresh the impacted services and create cases for the affected customers
- Correlate incidents with the open incidents or change requests using Agent assist
- Assign incidents and coordinate with network engineering

L1- Network engineer

The L1 - network engineer's tasks and responsibilities are as follows:

- Troubleshoot network incidents
- Engage Field Service agents, third-party vendors, and OEMs to resume normal service operation
- Trigger the Change Management and Problem Management processes

L2 - Network engineer

The L2 - network engineer's tasks and responsibilities are as follows:

- Troubleshoot network incidents
- Engage Field Service agents, third-party vendors, and OEMs to restore normal service operation
- Trigger the Change Management and Problem Management processes to introduce beneficial change or perform root cause analysis

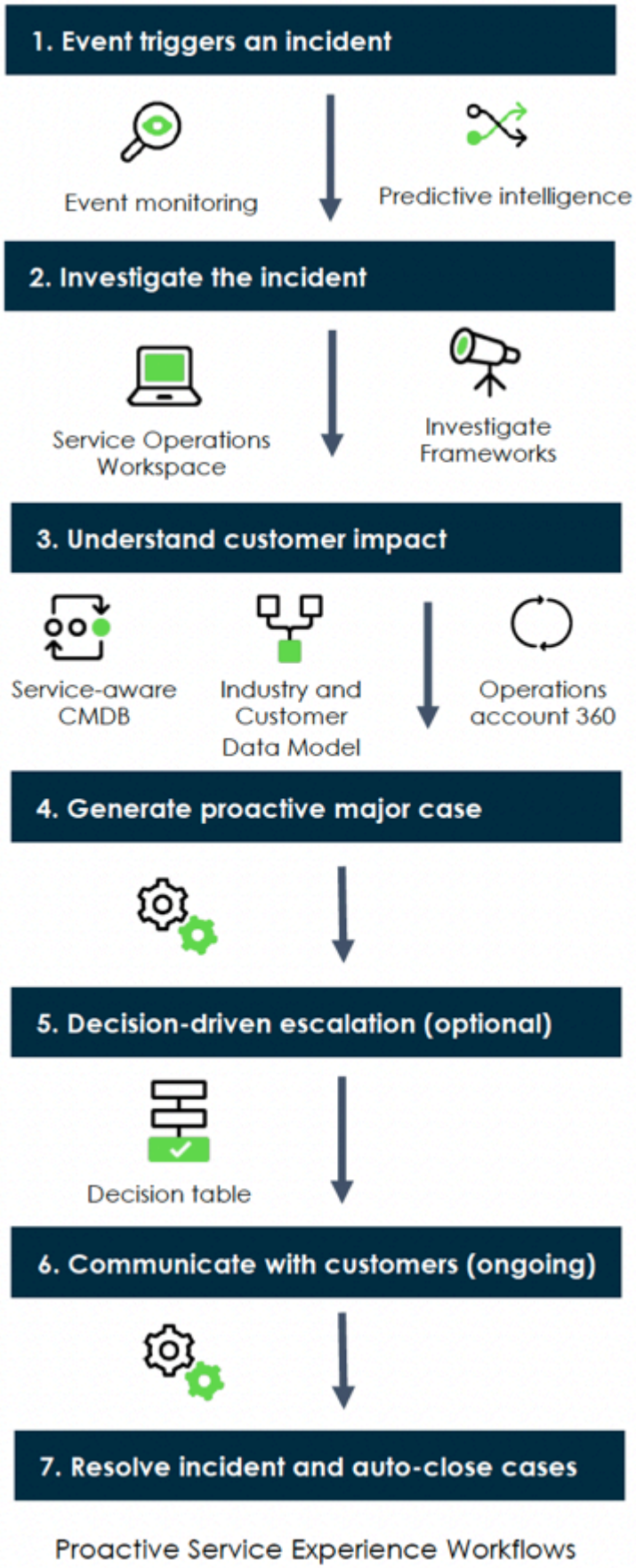
L3 - Network engineer

The L3 - engineer's tasks and responsibilities are as follows:

- Troubleshoot network incidents
- Engage Field Service agents, third-party vendors, and OEMs to restore normal service operation
- Trigger the Change Management and Problem Management processes to introduce beneficial changes or perform root cause analysis

Proactive Service Experience Workflows process

The following diagram shows the steps involved in the Proactive Service Experience Workflows process:



Proactive Service Experience Workflows

CMDB CI classes for Proactive Service Experience Workflows

Proactive Service Experience Workflows adds five Configuration Management Database (CMDB) configuration item (CI) classes that target the SD WAN edge infrastructure as part of the CMDB CI Class Models application.

Note:
To learn more about this application, see CMDB CI Class Models.

CMDB CI Classes for Telecommunications Assurance workflows

Class	Description	CI class extended
SD WAN Controller	Device that provides physical or virtual device management for all SD-WAN Edges	cmdb_ci_Server_Hardware
SD WAN Edge	Network functions (physical or virtual) that are located between the Underlay Connectivity service and the SD-WAN service	cmdb_ci_netgear
SD WAN Edge Port	Socket on a network device that connects to an external network	cmdb_ci_netgear
Network Circuit	Discrete path between two or more points that enable telecommunication connectivity services	cmdb_ci
Provider Edge	Point of connectivity between the SD WAN Edge Port and the service provider's core network	cmdb_ci_netgear

Proactive Service Experience Workflows and Incident Management within the Service Operations Workspace

You can use the Service Operations Workspace application to get an overview of how a network agent can prioritize tasks and resolve incidents.

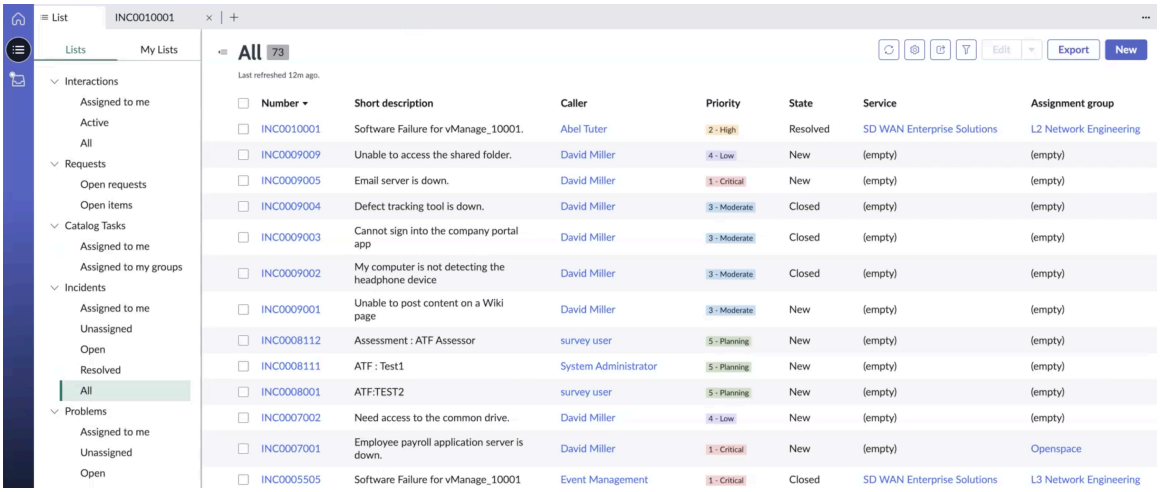
Viewing the Service Operations Workspace

From the **Workspaces** menu, select **Service Operations Workspace** and select the **Home** icon. From the landing page, a network agent can analyze incidents and view cases and upcoming tasks. To view:

- **Lists**: Select the **Lists** tab in the Service Operations Workspace. From the Lists tab, a network agent can analyze the individual lists of incidents and tasks and then take the appropriate action.

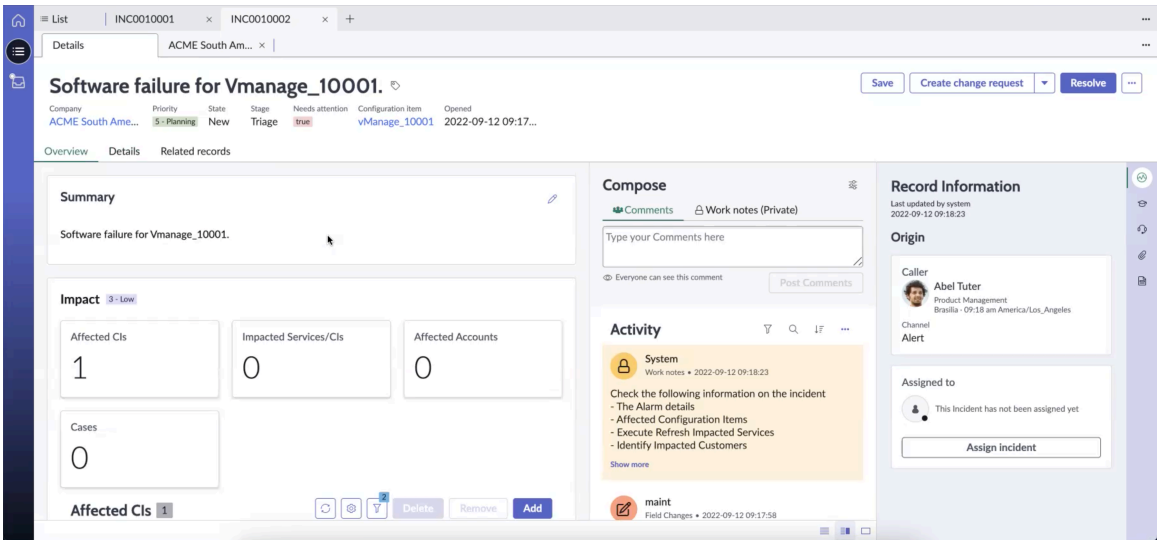
  The following example shows the List tab.

List tab



- Records: Open any task record to navigate to its record view as shown in the following example.

Record view



Example

The Proactive Service Experience Workflows application is automatically triggered when an incident is created within the system by an alert flow. A technical support can manually create this alert in the Service Operations Workspace. It can also be generated from an external fault management system using the TMF 621 integration.

The following example demonstrates how Proactive Service Experience Workflows is used to resolve an external network-initiated incident. In this example,

1. An external fault management system using TMF 621 integration sends an alert that triggers the creation of an incident record with the following values:
   - Short Description and Description: Vmanage_10001 failed to restart after a change was implemented.
   - Configuration Item: Vmanage_10001 (SD-WAN CI Class)
   - Category: SD-WAN

- Sub Category: Protocol Failure
- Affected Customers: 5

2. A technical support engineer opens the incident record inside the Service Operations Workspace and sees the list of impacted services and accounts in the **Overview** section.
3. The technical support engineer triages the issues by reviewing the latest changes in the Agent Assist that triggered the outage.
4. The technical support engineer then restarts the SD-WAN controller and selects **Generate Proactive Cases** in the Cases section. One major case and five child cases are generated and notifications are sent to the primary contacts for the affected accounts.
5. As a major case was created, the technical support engineer notifies the major issue manager of a potentially serious outage. The Major Issue Manager manages the major case record and communication with both technical teams and affected customers.
6. The Technical Support Engineer (TSE) realizes the device can't be rebooted and might have failed altogether. The TSE changes the Sub Category field to device failure and selects the **Escalate UI** action and enters a work note
7. The next level L2 Support team receives the incident and updates the record status.
8. The L2 Technical Support Engineer tries to troubleshoot the issues on the SD-WAN controller and successfully restarts the configuration item. Four out of the five the affected accounts report the issue is resolved, but the fifth account is still experiencing some problems.
9. To diagnose further issues with the fifth account, the L2 Technical Support Engineer performs the following steps:
   - Selects the check box next to the case record on the Overview page.
   - Selects the **Notify UI** action to send a message via additional comments to the contact person on the case record.
10. The contact person receives the additional comment and performs some extra steps. When the service is restored, the contact updates the status in the CSM portal.
11. Seeing the additional comments in the incident record, the L2 Technical Support Engineer changes the State field to **Resolved**.

    The resolution information is copied down to each case record, while the Major Issue Manager resolves the major case record and any associated cases.

Configuring Proactive Service Experience Workflows

You can configure Proactive Service Experience Workflows so that you can add users to assignment groups. You can also create custom instructions for engineers to guide them in resolving network-initiated issues through automatically provided workflows.

Install Proactive Service Experience Workflows

If you're a user with the system administrator role, you can install the Proactive Service Experience Workflows application.

Before you begin
Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.

- Role required: admin
- Plugins required: The following plugins must have been installed:
  - Customer Service Management
  - Customer Service with Service Management
  - Service Operations Workspace

About this task

The Telecom core application is installed with Proactive Service Experience Workflows:

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Proactive Service Experience Workflows application (sn_ind_tsm_sdwan) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you can't find the application, you may have to request it from the ServiceNow Store.

   Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.
3. In the Application installation dialog box, review the application dependencies.

   All dependent plugins and applications that are included, or must be installed are listed in the dialog box.
4. **Optional:** If demo data is available and you want to install it, select **Load demo data**.

   (Optional) Demo data comprises sample records that describe application features for common use cases. Load demo data when you first install the application on a development or test instance.

   Important:
   If you don't load the demo data during installation, it's unavailable to load later.
5. Select **Install**.

Add users to Proactive Service Experience Workflows assignment groups

Add users to Proactive Service Experience Workflows assignment groups so that they have the necessary role and can be assigned to resolve network-initiated issues at the appropriate escalation level.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. Select the group name.
   The four assignment groups are as follows:

- Network Coordinators
- L1 Network Engineering
- L2 Network Engineering
- L3 Network Engineering

3. In the Group Members related list, select **Edit**.
4. Select one or more names in the Collection list.
5. Select **Add**.
6. Select **Save**.

Using Proactive Service Experience Workflows

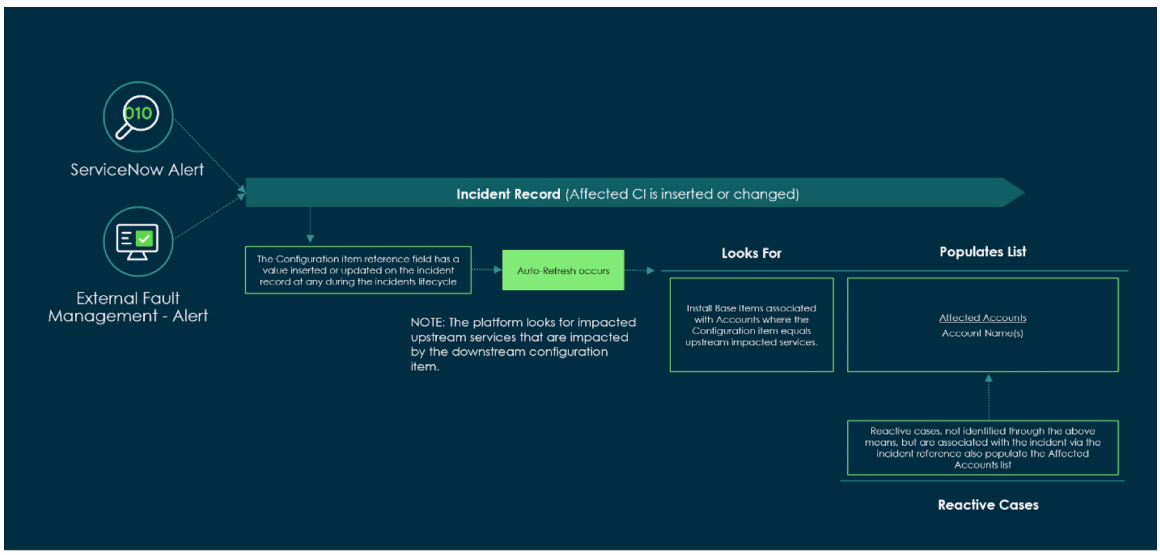
By using Proactive Service Experience Workflows, you can help resolve network-initiated incidents and proactively notify impacted customers. This application enhances the Incident Management application for common SD-WAN service issues that are detected by network management systems.

About identifying affected accounts with Proactive Service Experience Workflows in Incident Management

An incident record is created when an event management system generates an alert and the affected accounts can be viewed in the Service Operations Workspace.

When the technical support engineer logs in to the Service Operations Workspace, the affected configuration item, services, and customers are listed in the Overview section. These details are automatically updated when the Configuration Item in the Incident record is updated. When the Configuration Item is updated, the **Refresh Impacted Services** script is automatically triggered and retrieves services that are experiencing an outage or degradation. The impacted services associated with the accounts are identified and updated. Additionally, if a CSM agent associates a case with the incident record, the Affected Account list is also updated. When the Affected Account list is updated, the customer impact is visible to the support teams working on the incident record.

The following diagram shows the steps involved in creating an incident record.



Note:
The Change Management workflow follows the same process. When a configuration item is updated in a change request record, the **Refresh Impacted Services** script is triggered and the affected accounts are retrieved. Since the configuration item field is set to read-only, you must ensure that this field is populated before the script is triggered. See Create a case from a change request for more details.

Create an incident in Proactive Service Experience Workflows

Create an incident record in Proactive Service Experience Workflows to document an issue that your customer is facing.

Before you begin

Role required: sn_ind_tsm_sdwan.PSEW_USER, admin

Procedure

1. Navigate to **Workspaces** > *Service Operations Workspace* > **Incidents** > **All**.
2. From the incident list view, select **New**.
3. On the form, fill in the fields.

Incident form

Field	Description
Short description	Brief description of the incident.
Description	Detailed explanation of the incident.
Number	Unique system-generated incident number.
Company	Customer account that faced a network issue.
Caller	User who contacted you about an issue.
Location	Location of the caller.
Channel	Communication method that is used to create the incident. The available options are: ○ Chat ○ Email ○ Phone ○ Monitoring ○ Self-service ○ Virtual agent ○ Walk-in
State	State of the incident through several stages of resolution.
Impact	Measure of the effect of an incident or problem.
Urgency	Measure of how long the resolution can be delayed until an incident or problem has a significant business impact.
Priority	Based on the impact, urgency, and how quickly the resolution can be completed.

Field	Description
Service	Affected business service.
Service Offering	Service offering that consists of one or more service commitments that uniquely define the level of service for the availability, scope, pricing, and packaging options.
Configuration item	Affected configuration item.
Assignment group	Group that works on the incident.
Assigned to	User who works on this incident. If the **Assignment group** changes, the **Assigned to** field is cleared.
Additional comments	More information about the issue as needed. All users who can view the incidents can see the additional comments.
Work notes	Information about how to resolve the incident, or the steps that were taken to resolve it, if applicable.
Category and Sub Category	Type of issue. After selecting the category, select the subcategory, if applicable.

4. Select **Save**.

Result
The incident is created.

Create cases from an incident record in Proactive Service Experience Workflows

Create cases from records so that you can identify and solve network issues for your enterprise customers.

Before you begin
This task assumes that a workflow has already been triggered and an assignment group has been assigned.

Role required: sn_ind_tsm_sdwan.PSEW_USER

About this task
After a workflow in Proactive Service Experience Workflows triggers, you can identify the customers and systems that are affected by the network issue. You can then either automatically create the individual cases for the impacted customers or create a major case and child cases for a larger number of affected customers.

Procedure
1. Navigate to the *Service Operations Workspace*, and select **List** > **Incidents** > **Open**.
2. Select an incident from the list.
3. **Optional:** In an existing incident, assign the incident.
4. See the affected configuration items (CIs) by selecting the **Affected CIs** card.
5. See the impacted services by selecting the **Impacted Services/CIs** card and selecting **Refresh Impacted Services**.

6. See the affected accounts by selecting the **Affected Accounts** card and selecting **Identify Affected Accounts**.

   The ServiceNow® instance initiates an action to refresh the impacted services and to find the affected accounts.

7. Look for the names of the customers who are affected by selecting the **Affected Accounts** card and checking the Name column.
   Typically, the network coordinator creates cases so that the impacted customers are proactively notified of the network-initiated issues.
8. Generate proactive cases for the affected customers by selecting the Cases card and selecting **Generate Proactive Cases**.
   - If the number of affected accounts is less than the threshold, then this action creates one case for each affected account. Otherwise, this action first creates a major case and then creates child cases (one case for each affected account).
   - If you want to change the threshold, contact your administrator to change the value of the *sn_ind_tsm_core.major_case-affected_account_threshold* system property.
   - In the **Cases** tab, the major case is indicated by **[empty]** in the Account and Contact columns. Cases where that information is populated are child cases of that major case.
9. Create an ad-hoc case by selecting a case from the list and selecting **New**.
10. Notify a customer by selecting a case and selecting **Notify Customers**.
11. In the Notify Customers pop-up window, enter a descriptive note, and select **Notify**.

    A note is automatically inserted in the **Activity** field of the incident record and also in the selected cases record. If your customer updates the case with any message, it automatically synchronizes with the Incident record too.

    Note:
    By default, the Notify Customers functionality isn't active. As an admin, you must set the property value *proactive_workflows_for_providers.additional_comments_sync* to TRUE. Turn off the BR (business rule) *Update case worknote for comments change* to enable this functionality.

12. If you want to update the probable cause of the incident, select the **Cause** tab and save your message.
13. Resolve an incident by selecting **Resolve** on the incident record.
    In the Resolve pop-up window, enter the resolution code and resolution notes and select **Resolve**.

    Note:
    Only minor cases are automatically closed. For major cases, you must manually close all the related cases.

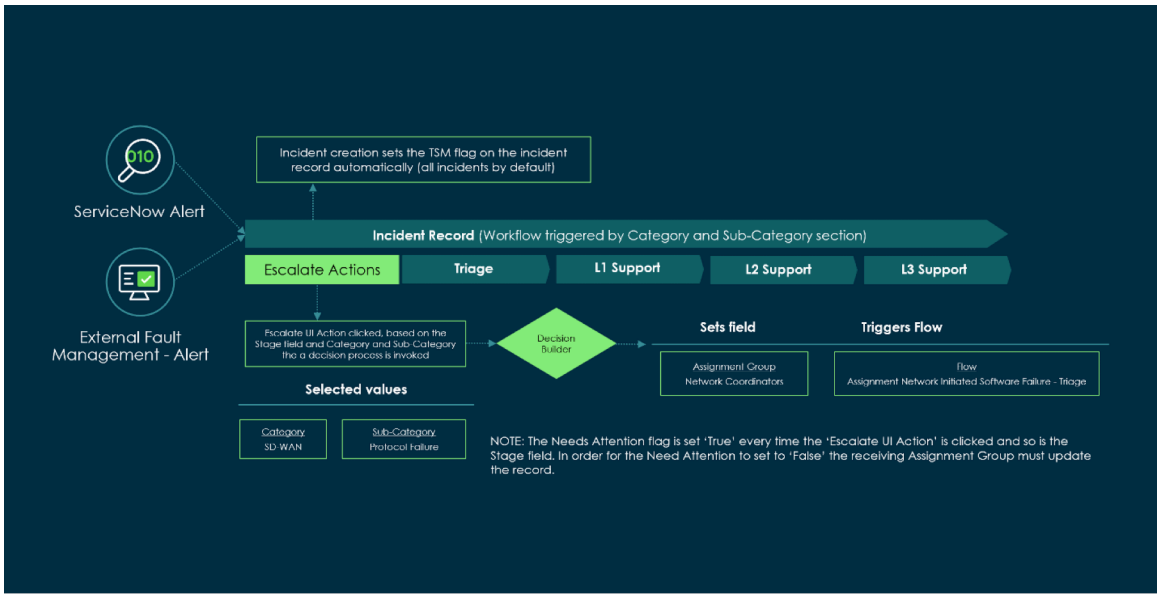
Result
When the incident is resolved, it triggers the auto-closure of related cases.

- If there's no major case, all the related individual cases are resolved and are updated with the work notes. The following field values from the parent incident record are also populated in the related cases:
  - Resolution Notes
  - Resolution Code
  - Probable Cause
- If there's a major case, the related cases don't get auto-resolved and a message is added to the work notes of the incident record, "There is a major case associated with this incident."The following field values from the parent incident record are populated in all the related major and child cases:
  - Resolution Notes
  - Resolution Code
  - Probable Cause

About escalating incidents

An escalation can be triggered when an incident is created with the appropriate category and sub category and the **Escalate UI** option is triggered within the Service Operations Workspace.

The following diagram provides a visual representation of the escalation flow.



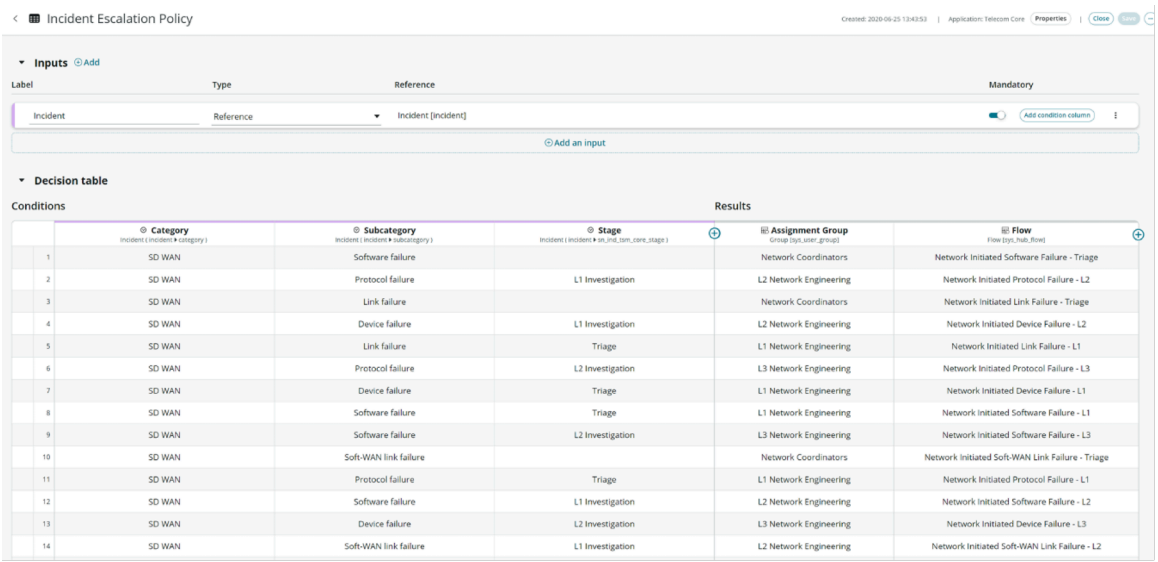
The following category and sub category values are available with the base system:

- Category: SD-WAN
- Sub category:
  - Link failure
  - Device failure
  - Protocol failure
  - Soft-WAN link failure
  - Software failure

The following values are available for the Stage field in the Incident table:

- Triage
- L1 investigation
- L2 investigation
- L3 investigation

Based on the defined conditions, such as current stage, category, and sub-category, the Incident Escalation Policy decision table determines the results and the next escalation stage if appropriate.


Incident Escalation Policy

Inputs Add

Label	Type	Reference	Mandatory
Incident	Reference	Incident (incident)	

Add an input

Decision table

Conditions | Results

	Category	Subcategory	Stage	Assignment Group	Flow
1	SD WAN	Software failure		Network Coordinators	Network Initiated Software Failure - Triage
2	SD WAN	Protocol failure	L1 Investigation	L2 Network Engineering	Network Initiated Protocol Failure - L2
3	SD WAN	Link failure		Network Coordinators	Network Initiated Link Failure - Triage
4	SD WAN	Device failure	L1 Investigation	L2 Network Engineering	Network Initiated Device Failure - L2
5	SD WAN	Link failure	Triage	L1 Network Engineering	Network Initiated Link Failure - L1
6	SD WAN	Protocol failure	L2 Investigation	L3 Network Engineering	Network Initiated Protocol Failure - L3
7	SD WAN	Device failure	Triage	L1 Network Engineering	Network Initiated Device Failure - L1
8	SD WAN	Software failure	Triage	L1 Network Engineering	Network Initiated Software Failure - L1
9	SD WAN	Software failure	L2 Investigation	L3 Network Engineering	Network Initiated Software Failure - L3
10	SD WAN	Soft-WAN link failure		Network Coordinators	Network Initiated Soft-WAN Link Failure - Triage
11	SD WAN	Protocol failure	Triage	L1 Network Engineering	Network Initiated Protocol Failure - L1
12	SD WAN	Software failure	L1 Investigation	L2 Network Engineering	Network Initiated Software Failure - L2
13	SD WAN	Device failure	L2 Investigation	L3 Network Engineering	Network Initiated Device Failure - L3
14	SD WAN	Soft-WAN link failure	L1 Investigation	L2 Network Engineering	Network Initiated Soft-WAN Link Failure - L2

The decision table is provided with the Proactive Service Experience Workflows application. You can modify the conditions that have been defined, and the results to suit your requirements. For more details on updating decision tables, see Decision Tables.

When an incident is escalated, the status of the Needs attention field is updated to **True**. The status can be changed to **False** by the owner of the Assignment Group field.

Note:
As a system administrator, you can configure the **Set Needs Attention False** business rule.

Escalate an incident in Proactive Service Experience Workflows

Escalate an incident to continue the investigation and diagnosis of that incident. By escalating an incident, you can ask for help from a more-experienced resource so that the issue is resolved more quickly.

Before you begin

This task assumes that you have been working on an incident and you must escalate it to the next escalation group.

Note:
Be sure that the administrator has assigned this role to the escalation groups. For information about how administrators assign roles, see Assign a role to a group.

Role required: sn_ind_tsm_core.noc_agent

Procedure

1. In the *Service Operations Workspace*, navigate to **List** > **Incidents** > **Open** and select an incident.
2. On the incident record form, from the drop-down list at the top-right corner, select **Escalate**.
3. In the Capture notes for the escalation pop-up window, enter a descriptive note and select **Escalate**.
   This action triggers the subflow for the next level of escalation group, and the Assignment Group automatically changes to the next escalation group.

Result

- The state of the incident task for the previous engineer is set to Closed Complete and the work note is logged.
- An incident task is created for the newly assigned user with the state set to Work in Progress.
- A work note in the activity stream provides instructions for the engineer at this level of escalation.
- The incident Stage is updated with the next escalation level.
- The Assignment Group is updated according to the escalation level.

Reviewing customer or partner accounts in Proactive Service Experience Workflows

Learn how your Technical Support teams (e,g. Cloud Ops, Server, or Network operations teams) can use the Operations Account 360 view in the Proactive Service Experience Workflows application to get insight about your customer's or partner's accounts.

As a technical support agent, you can collect information related to tasks, escalations, key customer data, and metrics associated with your customer's or partner's accounts in the Service Operations Workspace. With this data, you can track the following types of information:

- Who the customer or partner is and what products, services, assets, and configuration items have been sold to them.
- Who the key contacts are for both for the technology provider and customer or partner.
- What CSAT score is for the technology provider and customer or partner.
- How the technology provider and customer or partner are tracking from an SLA perspective for the month.
- What major incidents, cases, and escalations are affecting the accounts.
- How many tasks are being closed, by type, and how many are being opened on a rolling 12-week basis.
- Specific knowledge articles and catalog items developed for the account. With this information, your agents can gain the insights into what the customer or partner wants and what actions need to be taken.

The data visualized inside of Operations Account 360 view inside of Service Operations Workspace is derived from task records where the company value equals to the account selected when this view is launched. Knowledge Articles and Catalog Items are exception to this as.

Additionally, the Operations Account 360 View only works for company records with the class value equals to account. Company records with the class value of company shows the traditional default workspace view of Service Operations Workspace.

To learn more about getting the account insights, see Review an account by using the 360 View in Proactive Service Experience Workflows.

Review an account by using the 360 View in Proactive Service Experience Workflows

Review a customer or partner's account by using the Operations Account 360 view provided by the Proactive Service Experience Workflows application inside of Service Operations Workspace. You can track your data and tasks related to customer's or partner's and then take action to improve your delivery of service.

Before you begin

Role required: sn_ind_tsm_core_noc_agent

Procedure

1. Navigate to **Workspaces** > **Service Operations Workspace**.
2. From the Service Operations Workspace **Lists** tab, click **Accounts** > **All**.
3. In the Accounts list, select a customer account.

   Note:
   You can also access this view by clicking a company (account) name account inside the various incident lists or within the incident form in Service Operations Workspace.

4. In the Account Information page, in the Customer Summary section, review the general customer details for the selected account, such as Active status of the customer, Rank tier, and the number of employees.

   If this account has any escalations, you can view it by clicking **View Escalations**. In the Overview section, view the insights into account information.

Account Information page - Account Overview tab

Field	Description
Account Team Members	Team members of this customer. Click **View all** to see the list of all the team members.
Key Customer Contacts	Important contacts of this customer. Click **View all** to see the list of all the key customer contacts.
Single Score Cards	○ Contracts ○ Entitlements ○ CSAT **Note:** Results are from the assessments tied to the out-of-the-box Customer Satisfaction Survey provided by the Core CSM plugin. ○ Escalation Cases ○ Sold Products ○ Install Base

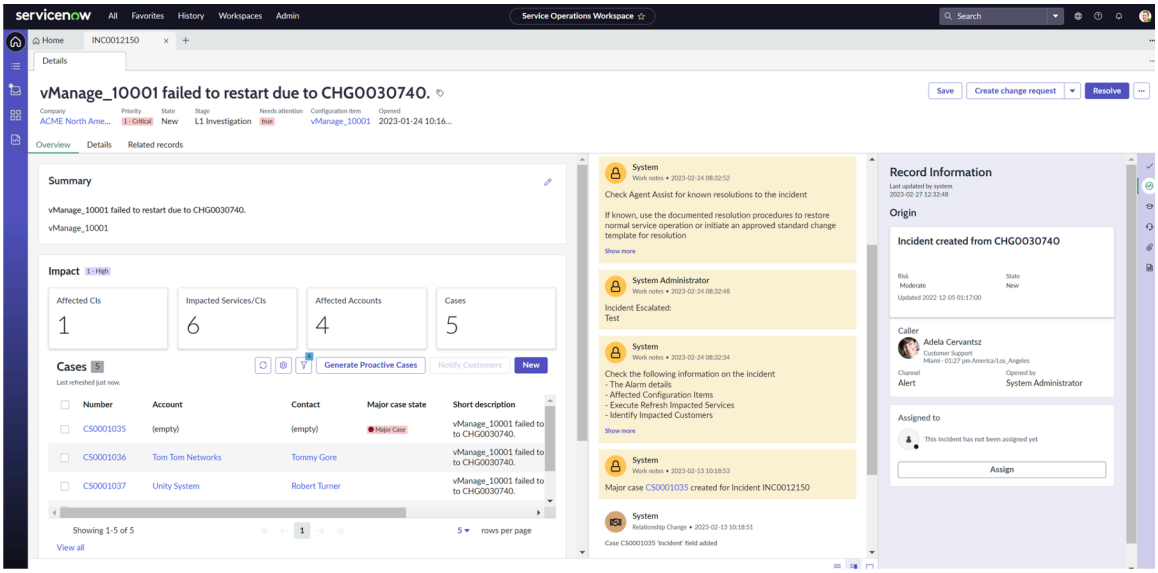
Field	Description
	○ Assets ○ Configuration Items
On-going Technical Support Work	○ Closed Tasks ○ Weekly New Tasks vs Closed Tasks ○ Current Month Task SLA Achievement
Changes	Change requests raised by your account
Problems	Problems related to the account
Incidents	Incidents related to the account
Incidents SLA	Incident SLAs related to the account
Outages	Outages related to the account
Requests	Requests related to the account
Cases	Cases related to the account
Contextual Side-panel	○ Attachments ○ Templates ○ Account Assist **Note:** You can also search for Major Incidents, Major Cases, Knowledge, Articles, or Catalog Items.

5. In the Related Records page, the default lists provided are:
   - Users
   - Contacts
   - Account Addresses
   - Product Models
   - Vendor Catalog Items

Auto creation of cases and updates from incidents

Cases are automatically created from incidents when the **Generate Proactive Cases** flag is selected.

A case is designated as a major case based on the value specified in the `major_case_affected_account_threshold` system property. This value can be modified by the administrator.



Depending on the threshold value, different flows are triggered to either create one major incident, or several individual cases. The case record is then populated. For example, in minor case scenarios, the following information is populated:

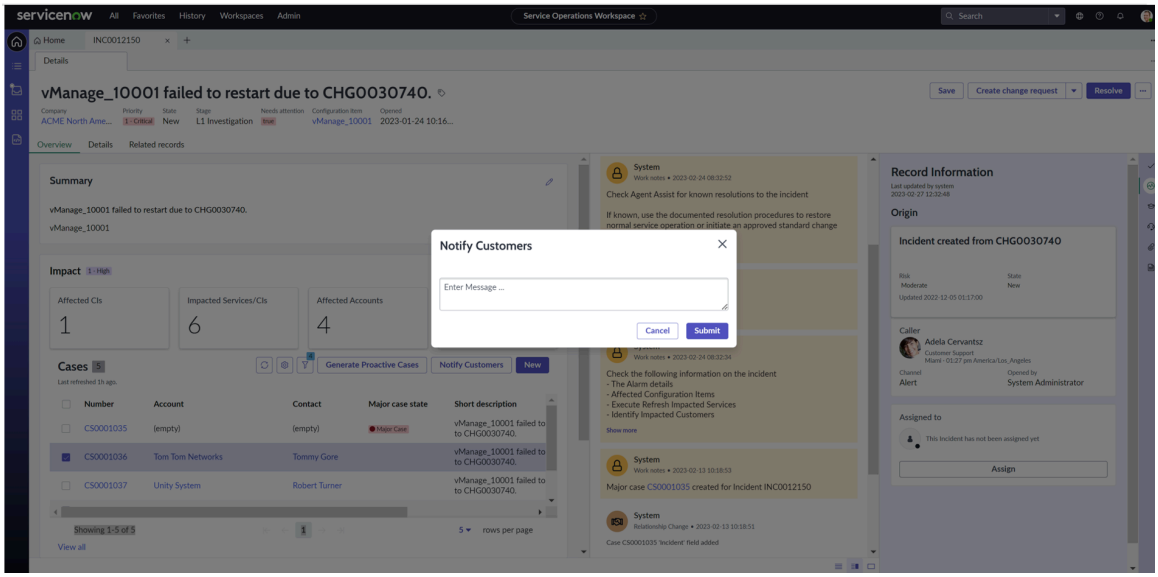
- Short description
- Description
- Proactive is true
- Channel
- Incident
- Account field

The administrator can specify the fields that must be passed to the case records from the parent incident record to suit their business needs.

Notify case information to customers

In the Service Operations Workspace, you can select one or more cases from the Cases section and select **Notify Customers**.

Enter your notification message and select **Submit**. The message is included under the Additional comments section with the case record and sent to the customer. When a customer responds to those comments either via an email, or from the CSM portal, these comments are copied to the incident record. The technical support engineer can view the response or any other feedback provided while reviewing the case.



Note:

To enable this feature, follow these steps:

- In the application navigator, type `sys_properties.list`.
- Search in the text field for the `proactive_workflows_for_providers.additional_comments_sync` system property.
- Select the system property to open the record.
- Enter **true** in the Value field and select **Update**.

To prevent additional comments from being copied to all cases related to the incident, deactivate the **Update case worknote for comments change** business rule in the incident table.

Setting major case threshold for auto generated cases

Set the threshold value for major cases generated from incidents in the system properties.

Before you begin

- Role required: admin
- Selected application scope: Telecom Core

About this task

A default threshold value has been predefined to generate major cases from incidents. This value may be too low or your organization may not be using the CSM major case management feature. In such cases, you can modify the threshold value in the system properties after the Proactive Service Experience Workflows has been enabled.

Procedure

1. In the Application Navigator, type, `sys_properties.list`.
2. Search in the text field for `major_case_affected_threshold` system property.
3. Click the system property to open the record.
4. Change the threshold number in the Value field.

Note:
The lower the integer value, the higher number of cases needed to trigger a major case. If a higher number is specified, the inverse is true.

5. Click **Update**.

Create a case from a change request

Create a case from a change request in Proactive Service Experience Workflows so that you can notify your customers about a service outage and its resolution after the change implementation is complete.

Before you begin

A change workflow has been triggered. An assignment group with the planned start and end dates have already been set.

Role required: admin

About this task

After a change workflow in Proactive Service Experience Workflows is triggered, you can identify the customers and systems that are affected by the change request. You can then either automatically create the individual cases for the impacted customers or notify your customers about the outages.

Procedure

1. In *Service Operations Workspace*, navigate to **List** > **Changes** > **Open** and select a change record.
2. **Optional:** In an existing change record, assign the change request to a support engineer.
3. Expand the Scope and impact section and select the **Affected CIs** card.
4. See which services are impacted by selecting the **Impacted Services** card and then selecting **Refresh Impacted Services**.

   The instance initiates an action to refresh the impacted services and to find the affected accounts.
5. See the list of outages by selecting the **Outages** card.
6. See which accounts are affected by selecting the **Affected Accounts** card.
7. In the Details section, change the state of the Change record to **Authorize**.
   The cases for the affected customers are automatically created.
8. Select a case from the list of created cases and then select **New**.
9. Notify a customer by selecting the customer's case and selecting **Notify Customers**.
10. In the Notify Customers pop-up window, enter a descriptive note about the case, and select **Notify**.

    A note is inserted automatically in the **Activity** field of the change record and in the selected case records. If your customer updates the case with a message, the case automatically synchronizes with the change record.

Note:

By default, the Notify Customers functionality isn't active.
As an administrator, to make it active, you must set the *proactive_workflows_for_providers.additional_comments_sync* property value to TRUE and then select *Update case worknote for comments change*.

11. When the change manager authorizes the change record and the status changes to **Scheduled**, you can update the state by selecting **Implement**, selecting **Review**, and then saving the record.
12. Select the resolution code from the drop-down list, enter the resolution notes before closing the change request, and update the state by selecting **Close**.

About messages used in escalation workflows in Proactive Service Experience Workflows

Multiple messages that are used within the incident escalation flows are available with the base Proactive Service Experience Workflows application.

These messages provide instructions to technical support engineers to troubleshoot, escalate, and resolve incidents. The ones provided with the base system address common network initiated incidents, but can be modified for your troubleshooting processes.

Customize message files for Proactive Service Experience Workflows

Customize the messages that provide instructions to the network engineers that are working on network-initiated issues for different subcategories, levels of escalation, and personas in Proactive Service Experience Workflows.

Before you begin

Role required: admin

About this task

Each subflow in Proactive Service Experience Workflows references a message file that provides instructions for agents to use to troubleshoot, escalate, and resolve network-initiated incidents. You can use the default message text, or customize the text for your internal troubleshooting processes.

Procedure

1. Navigate to **All** > **System UI** > **Messages**.
2. Search for key values that contain `sd_wan`.
3. Select the record with the text that you want to customize.
4. In the **Message** field, provide instructions for that subflow's subcategory, persona, and level of escalation.
5. Select **Update**.

Handling trouble ticket notifications

Use the Telecommunications trouble ticket notification to inform third-party systems about the incidents or cases that are created in a reactive or proactive way in the ServiceNow instance. The customer will receive notifications regarding updates on the incident.

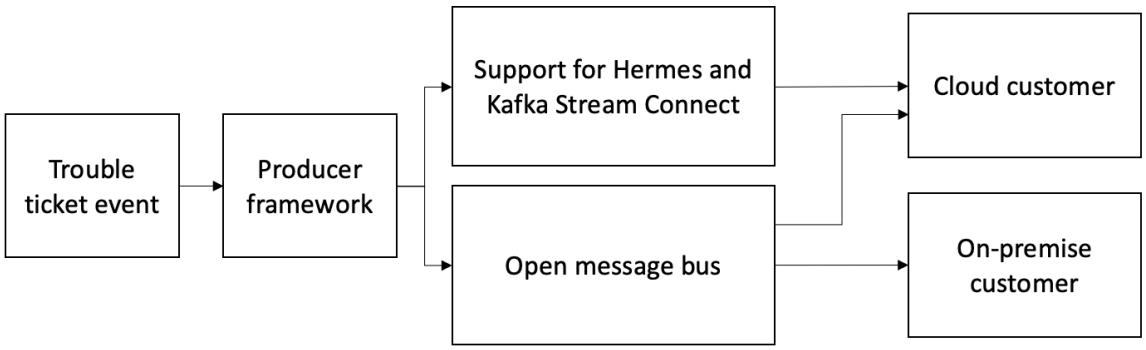
Overview

Trouble ticket in the TMF ecosystem is an incident that tracks and resolves customer-reported issues, network outages, or other problems. A trouble ticket incident can be created in either the reactive or proactive way. In the reactive approach, an incident is generated after conducting root cause analysis (RCA) on a case that is reported due to a system fault. In the proactive approach, an incident is generated after receiving alerts, enabling for the performance of RCA or service impact analysis (SIA) to evaluate the impact on the services. With the trouble ticket notification feature, you can send the details of the incident to the outbound systems.

Trouble ticket notification framework

The following diagram shows the components in the framework for the trouble ticket notification.

Trouble ticket notification data model



The trouble ticket notification uses a generic framework to send the outbound notifications to the external system. This framework supports two use cases:

1. Publish messages to Hermes Kafka using the Hermes messaging service. The cloud customers who use the Hermes Kafka can use this architecture to receive the notification.

   To learn more, see Producing outbound trouble ticket notifications using Hermes.

2. Publish messages to open message bus. This use case is message-bus agnostic and therefore supports publishing the notification to any open message bus. Both cloud and on-premise customers can use this use case. To learn more, see Producing outbound trouble ticket notifications using the open message bus.

Producing outbound trouble ticket notifications using Hermes

Produce an outbound notification from the ServiceNow instance using the Hermes capability. Customers can consume the details of the message from the Kafka environment in their external system.

Overview

In this use case, the notifications are produced to the Hermes cluster from your ServiceNow instance. After replication from Hermes to Kafka is completed, customers can consume or pull the messages from their own Kafka.

- To learn more about Hermes Messaging Service, see Hermes Messaging Service.
- To learn more about Apache Kafka Stream Connect, see Using Stream Connect for Apache Kafka.

In the Washington DC release, the following events are supported for trouble ticket notification.

- Create Trouble Ticket Event
- Trouble Ticket State Change Event
- Trouble Ticket Attribute Change Event
- Create Trouble Ticket Event for Case

Prerequisites

Before producing an outbound notification, the customer must create the topic in the Hermes cluster. To learn more about creating a topic in Hermes, see Managing namespaces and topics in Hermes.

Workflow

The workflow for producing the outbound notification by using Hermes contains the following steps:

1. On the trigger of the trouble ticket event, the system invokes the appropriate business rule, and stamps the event type.

   To learn more about business rule that you must add to your ServiceNow instance, see Add a business rule for a new trouble ticket event.

2. The system pushes the Glide snapshot and event type in the staging table, which acts as a queue.
3. The producer framework picks the event and converts it to a TMF 688 complaint event payload.

   To learn more about the system properties that you must configure for the producer framework, see Using the producer framework for outbound notifications.

4. The system invokes the Producer V2 API of Stream Connect and produces the event on the Hermes Kafka topic.
5. The Stream Connect pushes the event in the Hermes Kafka cluster.
6. The customers can consume the message in their in-house Kafka.

Related topics

EventProcessorUtilOOB - Scoped

EventQueueProcessorOOB - Scoped

Producing outbound trouble ticket notifications using the open message bus

Produce an outbound notification from the ServiceNow instance using the open message bus. Customers can consume the details of the notification from the message bus in their external system.

Overview

In this event-driven architecture, the notifications are produced to the open message bus from your ServiceNow instance. The framework contains topic synchronization and topic picker mechanisms. The topic synchronization mechanism synchronizes the topics that you have created in the ServiceNow instance with the open message bus. When the event occurs in the framework, the topic picker mechanism picks the relevant topic and publishes the message to the topic using a REST proxy. Customers can consume the outbound notification from the message bus in their external system.

In the Washington DC release, the following events are supported for trouble ticket notification.

- Create Trouble Ticket Event
- Trouble Ticket State Change Event
- Trouble Ticket Attribute Change Event
- Create Trouble Ticket Event for Case

Prerequisites

Before producing outbound notifications, it's necessary to create the egress topics on the Topic [sn_api_notif_mgmt_topic] table in the ServiceNow instance. When you create an egress topic, the system runs a business rule and attempts to synchronize the topic to the message bus based on configuration. To learn more about manually creating a topic in the Topic table, see Create a topic. The system synchronizes only the egress topic with the message bus in the external system. The **user_created** field in the associated topic record is set to true.

Alternatively, you can create the topics on the message bus in your external system and push them into the Topic table in ServiceNow instance. The customers invoke the `Event Management Topic Open API` endpoint, which stores the topic in the Topic [sn_api_notif_mgmt_topic] table of ServiceNow instance. The **user_created** field in the associated topic record is set to false. To learn more about the methods that are used when processing the `Event Management Topic Open API` endpoint, see Event Management Topic Open API.

Workflow

The workflow for producing the outbound notification by using the open message bus contains the following steps:

1. On the trigger of the trouble ticket event, the system invokes the appropriate business rule, and stamps the event type.

   To learn more about the business rule that you must add to your ServiceNow instance, see Add a business rule for a new trouble ticket event.

2. The system pushes the Glide snapshot and event type in the staging table, which acts as a queue.
3. The producer framework picks the event and converts it to a TMF 688 complaint event payload.

   To learn more about the producer framework, see Using the producer framework for outbound notifications.

4. The topic picker mechanism determines the topics, which are compatible with the event type. Topic picker performs the following steps to check the compatibility of the topics:

   a. The System scans the topics that have the **Type** field set as **Egress** in the topic table.

   b. The system checks the header query and content query of all egress topics and matches the compatibility with the event payload.

   To learn more details about how to customize the existing topic picker mechanism, see OpenMessageBusEventPublisherOOB - Scoped.

5. The system sends the list of compatible topics and event payload to the spoke selector.
6. The spoke selector, which the customer has configured, invokes the REST step that is configured for each topic and sends to the message bus REST Proxy in the external system.

To learn more about the method for sending messages to the spoke selector, see OpenMessageBusEventPublisherOOB - Scoped and Configure the Producer Event Notification Framework to use the Open Message Bus.

7. The customers can consume the message in their message bus REST Proxy.

Related topics

EventProcessorUtilOOB - Scoped

EventQueueProcessorOOB - Scoped

Handling the external events using Telecommunications API notification

Using the producer framework for outbound notifications

The producer framework picks the event from the ServiceNow instance and sends the outbound notification to the external system. You can consume the details of the notification from the messaging service that is installed in your external system.

System properties

You must configure the system properties to use the producer framework for outbound notification. The following table explains the list of system properties that are set for the scheduled jobs.

Producer framework system properties

Property	Description	Type
sn_api_notif_mgmt.event.log	Level of logging to be written to the debug logs. You can select the following logging levels: • **emerg**: Total failure. • **alert**: System corruption of a database, for example. • **crit**: Typically used for hardware errors, for example. • **err**: Any errors. • **warning**: Any warnings • **notice**: Possible action required but not essential. • **Info**: No action required. • **debug**: Generally not used except for capturing everything for fault-finding. Default value: **err**	String
sn_api_notif_mgmt.publisher_messages_with_configs	Defines whether messages are published using the	String

Producer framework system properties (continued)

Property	Description	Type
	Hermes Messaging Service, the Open Message Bus, or both message buses. You can use the following values: • **openMessageBus** • **hermes** • **both** Default value: **openMessageBus**	
sn_api_notif_mgmt.inboundqueue.maxrecords	Maximum number of records that the scheduler will pull from the inbound queue for one scheduler run. This value is used in conjunction with the *sn_api_notif_mgmt.inboundqueue.batch.limit* parameter. • Default value: **200** • Other possible values: As needed For example, if the batch limit is set to 50 and the maxrecords is set to 200, and if the number of records that are in the inbound queue is 130, then the scheduler would pull three different batches of records in a single run; two with 50 records and one with 30 records. If the number of records in the inbound queue is 220, the scheduler would pull four batches of 50 records and the remaining 20 records would not be processed until the next time the scheduler runs. When setting this value, you must also consider the time that it will take for the scheduler to process multiple batches and set the sn_api_notif_mgmt.schedule.max.runtime value accordingly.	Integer
sn_api_notif_mgmt.inboundqueue.batch.limit	Number of records that the scheduler pulls and	Integer

Producer framework system properties (continued)

Property	Description	Type
	processes from the inbound queue at one batch. • Default value: **200** • Other possible values: As needed	
sn_api_notif_mgmt.glide.mutex.spin.max	Maximum number of attempts to acquire a mutex lock in the inbound queue records. • Type: Integer • Default value: **100** • Other possible values: As needed	Integer
sn_api_notif_mgmt.schedule.max.runtime	The maximum time, in milliseconds, that the scheduled job can run before it fails and reports an error. • Type: Integer • Default value: **90000** • Other possible values: As needed	Integer
sn_api_notif_mgmt.glide.mutex.spin.wait	Maximum wait time, in milliseconds, to wait between attempts to acquire a mutex lock on the records in the inbound queue. • Type: Integer • Default value: **100** • Other possible values: As needed	Integer

Producer framework workflow

When the system pushes an event to the staging table, the following steps take place as part of the producer framework mechanism:

1. The scheduler picks a number of records at a preconfigured interval and then sends Glide snapshots to the event processor.
2. The system converts the Glide snapshot to a TMF 688 complaint event payload based on the event type.

   To learn more about the methods used to define and generate the TMF-compliant payloads for trouble ticket events, see TopicAPIUtilsOOB - Scoped.

3. The system checks whether the notification configuration is intended for Hermes Kafka or the open message bus.

   To learn more about configuring the producer event notification framework, see Producer Event Notification Framework developer guide.

Related topics

Producing outbound trouble ticket notifications using Hermes

Producing outbound trouble ticket notifications using the open message bus

Deactivate trouble ticket notification

Disable the business rules related to the incident and case tables to stop receiving trouble ticket notifications. Customers can disable the business rules if they don't want to leverage the trouble ticket notification capability.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **System Definition** > **Business Rules**.
2. Select the following business rules, and deselect the **Active** check box.
   - Create Trouble Ticket Event
   - Trouble Ticket State Change Event
   - Trouble Ticket Attribute Change Event
   - Create Trouble Ticket Event for Case

Proactive Service Experience Workflows reference

Reference topics provide additional information about Proactive Service Experience Workflows.

Domain separation and Proactive Service Experience Workflows

Domain separation is supported for Proactive Service Experience Workflows. With Proactive Service Experience Workflows, you can quickly restore normal service operation when network-initiated incidents occur and proactively identify and notify the customers that are impacted by those incidents. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes **Basic** level support.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

Overview

Proactive Service Experience Workflows (TAW) is a series of workflows that enhance the Incident Management application and its integration with customer workflow processes, such as Case Management and Field Service Management. That means that Proactive Service Experience Workflows doesn't require any additional domain separation support because the foundation applications already provide that support. To learn more, see Proactive Service Experience Workflows.

Related topics

- Domain separation for service providers