



Washington DC Operational Technology Management

Last updated: 02/01/2024

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.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks
are trademarks and/or registered trademarks of ServiceNow, Inc., in
the United States and/or other countries. Other company and
product names may be trademarks of the respective companies
with which they are associated.

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

Operational Technology.....	5
Operational Technology Management licensing and subscriptions.....	7
Subscriptions for OTM.....	7
Install ITOM SU Licensing.....	8
View subscription statistics for OTM.....	9
Review OTM resource usage against allocated subscription units.....	9
Check CI count used for OTM subscriptions.....	10
View CIs consuming OTM subscription units.....	12
OTM SU Licensing References.....	13
Operational Technology Manager.....	16
Exploring the Operational Technology Manager.....	17
Configuring the Operational Technology Manager.....	27
Operational Technology Manager Integrations.....	31
Using the Operational Technology Manager.....	89
Operational Technology Manager reference.....	145
Industrial Process Manager.....	146
Exploring Industrial Process Manager.....	146
Configuring the Industrial Process Manager.....	148
Using Industrial Process Manager with the Operational Technology Manager.....	171
Industrial Process Manager reference.....	193
Operational Technology Vulnerability Response.....	195
Exploring Operational Technology Vulnerability Response.....	195
Configuring Operational Technology Vulnerability Response.....	209
Operational Technology Vulnerability Response Integrations.....	220
Using Operational Technology Vulnerability Response.....	238
Operational Technology Vulnerability Response reference.....	242
Operational Technology Incident Management.....	243
Exploring Operational Technology Incident Management.....	243
Configuring Operational Technology Incident Management.....	246
Using Operational Technology Incident Management.....	258
Operational Technology Incident Management reference.....	268
Operational Technology Change Management.....	269
Exploring Operational Technology Change Management.....	269
Configuring Operational Technology Change Management.....	272
Using Operational Technology Change Management.....	283
Operational Technology Change Management reference.....	297
Operational Technology Knowledge Management.....	298
Exploring Operational Technology Knowledge Management.....	298
Configuring Operational Technology Knowledge Management.....	299

Using Operational Technology Knowledge Management.....	307
Operational Technology Knowledge Management reference.....	313
Domain separation and Operational Technology.....	316

Operational Technology

Use ServiceNow® for Operational Technology to help your organization streamline operations, boost productivity, and maximize your Operational Technology uptime on the production floor through digital workflows.

Benefits in Operational Technology, Core Operations, and empowering Factory Workers



Operational Technology

Contextualize and safeguard your Operational Technology systems, connect to digital workflows, and respond quickly to threats.



Core Operations

Streamline and digitize standard operating procedures (SOPs) and enable shared knowledge and collaboration across the enterprise.



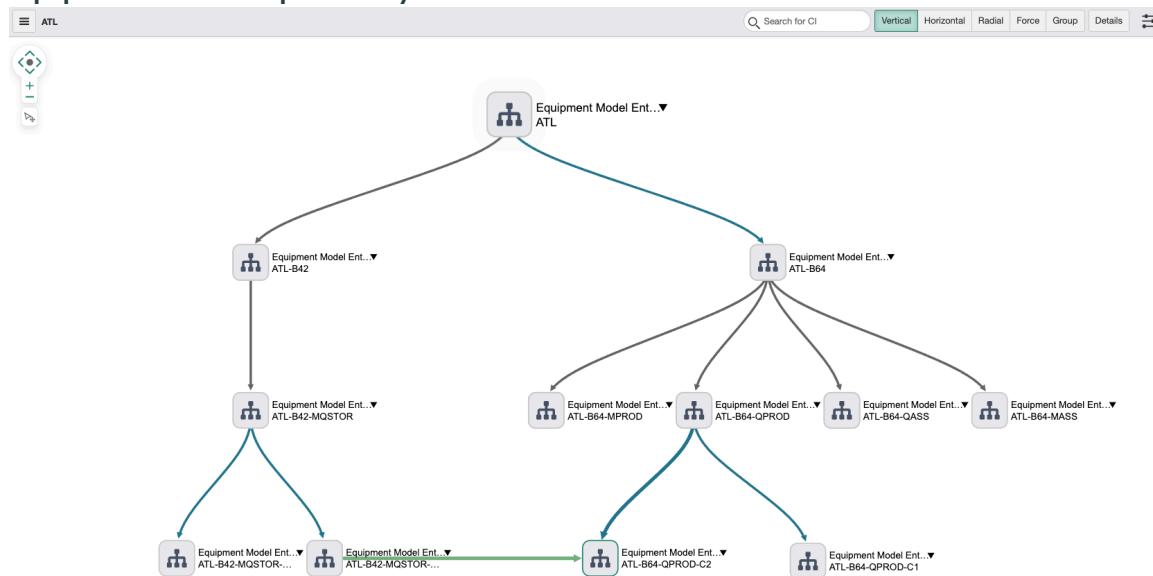
Factory Workers

Empower the workforce with digital tools and knowledge to adapt, collaborate, and excel in fast-changing conditions.

Maximize your uptime and build operational resilience with ServiceNow Operational Technology Management

Before industry Operational Technology, manufacturers depended on manual processes and legacy knowledge to maintain their environments. They found it challenging to get a complete view of their environments and to secure, monitor, and manage it all. With the ServiceNow Operational Technology Management solution, your industrial organization can now get a complete and contextual view of your operational technology systems. With this view, you can keep your systems secure, running, and connected to production processes and digital workflows. You can also enable your organization to assess, prioritize, and respond to events and threats.

Equipment model dependency view



By using a digital map, your organization can gain greater visibility of the industrial operations processes, systems, and relationships. With this map, you can manage and assess your potential production impacts easier and faster.

Improve visibility	 Get a complete and contextual view of your Operational Technology systems, so that you can keep your systems secure and running.
Digital workflows	 Connect your Operational Technology systems to production processes and digital workflows.
Vulnerability management	 See everything in one place, so that you can assess, prioritize, and respond to events and threats.

Equip your workforce

Build low-code and no-code applications so that your employees can do collaborative monitoring, extended troubleshooting, problem-solving, and in-depth situational analysis.

See the [solution brief](#)  for details.

Get started

- Watch features demonstrated via [DemoNow](#) .
- For information on how to request and set up Operational Technology, see
 - [Configuring the Operational Technology Manager](#)
 - [Configuring the Industrial Process Manager](#)
 - [Configuring Operational Technology Vulnerability Response](#)
 - [Configuring Operational Technology Incident Management](#)
 - [Configuring Operational Technology Change Management](#)
 - [Configuring Operational Technology Knowledge Management](#)
- For more information about how Operational Technology manages and uses Common Service Data Model tables, see [Operational Technology and CSDM tables](#) .
- For more information about the latest releases for Operational Technology, see [ServiceNow Store - Operational Technology release notes](#) .

Applications

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)
- [Operational Technology Vulnerability Response](#)
- [Operational Technology Incident Management](#)

- Operational Technology Change Management
- Operational Technology Knowledge Management
- Service Management: [IT Service Management](#)
- Security: [Vulnerability Response](#)
- Visibility: [IT Operations Management](#)

Operational Technology Management licensing and subscriptions

ServiceNow® OTM licensing is a crucial aspect of Operational Technology Management as it calculates and presents the usage of OTM subscriptions based on subscription units, which could encompass factors like the number of devices monitored or the duration of the subscription.

Overview

This enables organizations to ensure compliance, allocate resources effectively, and make informed decisions about scaling their OTM capabilities to safeguard their operational technology systems and adapt to changing security and operational needs. Use the OTM licensing module to access subscription-related details for the OTM products: ServiceNow OT Foundation, ServiceNow OT Visibility, and ServiceNow OT Vulnerability and Response.

Get started

<p>Explore OTM license</p>  <p>Learn about subscription-related details</p>	<p>Install ITOM SU Licensing for OTM</p>  <p>Update the latest version of plugin</p>	<p>Licensing References</p>  <p>Know about installed components like scheduled jobs and tables</p>
--	---	---

Contact Support

[Contact Customer Service and Support](#)

Subscriptions for OTM

The ServiceNow platform employs OTM for license management in the manufacturing sector. OTM encompasses licenses found in IT Operations Management, along with licenses exclusive to the OTM domain.

Monitor OTM licenses in a manner similar to IT Operations Management licenses. Within the ServiceNow instance, you can identify OTM license types on the **ITOM Licensing Category MetaData (OTM License > Licenses by CI types)** page, where the **SKU Type** column displays a value of **otm**. By default, the license filter is set to **SKU Type** contains **otm**.

Install ITOM SU Licensing

Install or update the ServiceNow® ITOM SU Licensing [sn_itom_licensing] to ensure you use the latest licensing functionality. The application includes demo data and installs related ServiceNow® Store applications and plugins if they are not already installed.

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](#).
- Review the [ITOM SU Licensing](#) application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.

Role required: admin

About this task

Prior to Q1 2022, the original licensing mechanism was delivered as part of the family releases. Since then the licensing mechanism is delivered using ServiceNow® ITOM SU Licensing on ServiceNow Store. The system automatically installs ServiceNow® ITOM SU Licensing. You receive notifications when updates for this application are available on ServiceNow Store.

The following items are installed with ITOM SU Licensing:

- Scheduled jobs
- Tables

For more information, see [Components installed with ITOM SU Licensing for OTM](#).

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.

2. Find the application (sn_itom_licensing) using the filter criteria and search bar.

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

In the list next to the **Update** button, the versions that are available to you are displayed.

3. Select a version from the list and select **Update**.

In the Install dialog that is displayed, any dependencies that are installed along with your application are listed.

4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.

5. Optional: If demo data is available and you want to install it, select the **Load demo data** check box.

Demo data comprises the sample records that describe application features for the common use cases. Load the 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.

6. Select **Update.**

View subscription statistics for OTM

View the count of OTM application subscriptions purchased and consumed by your organization, offering valuable insights for resource management and operational technology optimization.

Before you begin

- Ensure your organization has active OTM subscriptions.
- Ensure that you installed the latest available version of the ITOM SU Licensing from ServiceNow Store .

Role required: sn_itom_license.reader

About this task

Evaluate the allocation of configuration items (CIs) and their allocation levels to assess the OTM subscription utilization of your organization and to prepare for future subscription requirements.

Procedure

1. To view subscription information for OTM subscriptions purchased a la carte, navigate to **OTM License > License Summary**.
2. Review the details presented on the form, as outlined in the [Subscriptions form for the OTM products](#).

Review OTM resource usage against allocated subscription units

Review and analyze resource statistics that OTM products can manage and compare this information to the average allocation of subscription units.

Before you begin

Role required: admin

About this task

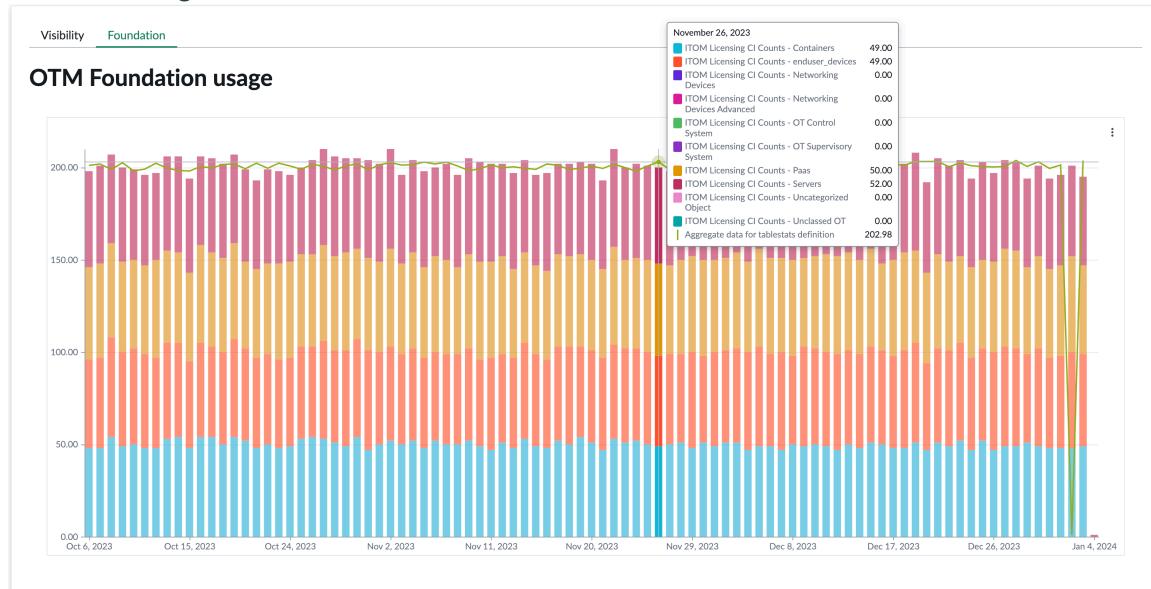
Explore detailed licensing data trends of OTM using the [OTM Licensing dashboard](#). Observe daily CI counts or view the averages for the last 90 daily counts. This feature provides domain-specific information and specific CI listings for each daily count, enabling you to effectively monitor and analyze resource usage over time.

Note: CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days.

Procedure

1. Navigate to **All > OTM License > OTM Licensing Dashboard**.
2. Select the relevant tab to display the dashboard for the OTM product.
For example, select **Foundation**.

OTM Licensing Dashboard



3. Point to a bar to view the number of CIs in each category.
4. Select the bar to view a list of the counted CIs.
5. Review the dashboard described in [OTM Licensing dashboard](#).

Check CI count used for OTM subscriptions

View the daily counts or the averages for the most recent 90 days of CI data. ServiceNow OT Foundation, ServiceNow OT Visibility and ServiceNow OT Vulnerability and Response offer insights into the licensed resources that OTM applications support. Resources that OTM applications discover, monitor, and provision are configuration items (CIs) stored in the CMDB. The OTM licensing module combines this CI information with the information on subscriptions your organization purchased to produce statistics on subscription use by OTM applications.

Before you begin

- Ensure your organization has active OTM subscriptions.
- Ensure that you installed the latest available version of the ITOM SU Licensing from [ServiceNow Store](#) ↗.

Role required: sn_itom_license.reader

About this task

ServiceNow incurs charges for the usage of ServiceNow OT Foundation, ServiceNow OT Visibility and ServiceNow OT Vulnerability and Response. To gain a deeper understanding of the products and features included in OTM subscriptions, see [Subscriptions for OTM](#).

The procedure for gathering and consolidating data for licensing purposes involves the following series of actions:

1. The OTM licensing system calculates the daily count of configuration items (CIs) managed by each OTM product, subsequently categorizing these CI counts into distinct licensable CI categories.
2. In cases where identical configuration items (CIs) are being managed by various features within the same OTM products, adjustments are made to eliminate any duplications in the CI count.
3. In cases where IT configuration items (IT CIs) are categorized as OT configuration items, the CIs are counted only once - under OTM licensing and not under ITOM licensing.
4. The licensing module consolidates CI counts from OTM applications to calculate the average of the daily CI count for the last 90 days.

i Note: CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days ago.

5. The licensing module matches the daily average CI counts for OTM applications with the licensing details provided in the customer contract to generate license-related statistics.

Consequently, you can view the statistics on how your organization utilizes the purchased subscription units.

View information on CI count and subscriptions purchased for each OTM application separately (a la carte):

- **Total Count:** The average of the CI counts collected over 90 days, categorized by CI types, for each individual OTM application.
- **Note:** CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days ago.
- **Subscription Unit Ratio:** Ratios determine how many CIs of a particular CI category necessitate a subscription. The licensing module retrieves this ratio information from customer contracts.
- **Total Subscription Units Consumed:** The quantity of subscriptions used by your organization for each CI category within each OTM application. This calculation is performed by applying the subscription units ratio to the count of CIs within each respective CI category.
- **Total Subscription Units Consumed:** The total subscription units consumed by all OTM applications combined.

You can access OTM Subscription Unit (SU) consumption categorized by domain. This data can be useful for allocating consumption and expenses to different organizations.

Procedure

1. Navigate to **OTM License > License Report.**

CI Category	Domain	Total Count	Subscription Unit Ratio	Total Subscription Units Consumed
Networking Devices	global	17	25:1	0
OT Control System	global	210	3:1	70
OT Field Device	global	19	10:1	1
OT Supervisory System	global	7	1:1	7
Servers	global	20	1:1	20
Unclassed OT	global	49	1:1	49
	Sum			147
	Sum			147

2. Optional: View the average of daily CI counts for the last 90 days.
3. Optional: To view the daily CI counts, modify the filter to set **Aggregated** to **false**.
(Optional) If needed, you can modify the view by sorting the columns. The **Created** column displays the timestamp indicating when the CI information was most recently updated.

View CIs consuming OTM subscription units

Generate a list of currently countable CIs for each of the OTM applications: ServiceNow® OT Foundation, ServiceNow® OT Visibility and ServiceNow® OT Vulnerability and Response.

Before you begin

- Ensure your organization has active OTM subscriptions.
- Ensure that you installed the latest available version of the ITOM SU Licensing from [ServiceNow Store](#).

Role required: sn_itom_license.reader

About this task

The CI list generated is strongly correlated to the most recent daily count of CIs. However, it's possible that the number of CIs on the generated list may display slight discrepancies compared to the latest daily count if any changes have occurred since the last daily count.

Procedure

1. Navigate to **All > OTM License > Report OTM Licensable CIs**.

The **Report ITOM Licensable CIs** page appears.

2. Select the application for which you want to see licensed CIs.
 - Foundation
 - Visibility
 - HLA
 - Health

Application	Max Results	Status	Progress	Additional Filters for CIs
Foundation	10,000	Completed	1/10000	
Health	10,000	N.A.		
Visibility	10,000	Completed	1/10000	
HLA	10,000	N.A.		

3. To create a report for the selected applications, select **Populate licensable CIs**.

4. To accept the confirmation message and generate the report, select **Yes**.

The new report replaces the data in the previously generated report. You can cancel the report by selecting the application and then opting for the **Cancel Job** option.

5. Wait for a few minutes and then refresh the page.

The application status is displayed as **Completed** once the report has finished processing.

6. Select the application and then select **Show licensable CIs**.

The ITOM Licensable CIs page for OTM SKU displays the list of CIs with an OTM license.

OTM SU Licensing References

Use reference topics to gain valuable insights on the components installed with OTM licensing, subscription forms for OTM products, and an overview of the OTM licensing dashboard. Navigate the subtopics to access specific guidance and references on each of these critical aspects, helping you effectively manage your OTM subscriptions and licensing requirements.

Components installed with ITOM SU Licensing for OTM

Several types of components are installed with activation of the OTM SU Licensing plugin, including scheduled jobs and tables.

Scheduled jobs installed

Scheduled job	Description
ITOM Exclusion Tables Update Store	Updates the exclusion list.
ITOM Licensing Aggregator Store	Calculates the average of daily CI counts for the last 90 days.
ITOMHealthCIReporterWithOTOMCountOTOMStore	Compiles the list of licensable CIs for OTM Health.
ITOM Health Licensing Usage Count Store	Calculates the daily CI count for OTM Health.
OTOM Licensing Visibility CI Listing Store	Compiles the list of licensable CIs for OTM Visibility.
OTM Foundation Licensing CI Listing Store	Compiles the list of licensable CIs for OTM Foundation.
OTM Foundation Licensing Usage Count Store	Calculates the daily licensable CI counts for OT Foundation.

Tables installed

Table	Description
ITOM LU Discovery Source Mapping [itom_lu_discovery_source_mapping]	Contains the list of licensable discovery source for each category.
ITOM LU Governance App Mapping [itom_lu_governance_app_mapping]	List of records that contain the mapping of governance applications to their respective licensable CIs.
ITOM LU Governance CIs [itom_lu_governance_ci]	Contains the list of CIs counted under the Governance license.
ITOM License Exclusion Metadata [itom_license_exclusion_metadata]	Contains the list of exclusion rules applicable to different license.
License Exclusions	Contains the list of CIs that need to be excluded from the license count based on the exclusion rule.

Table	Description
[license_exclusion_list]	
Visibility LU Temporary [visibility_lu_temp]	Contains the list of Cls counted under the Discovery license.
ITOM Licensing Category MetaData [itom_lu_category_metadata]	Contains licensing metadata.
ITOM Licensing Discovery Sources [itom_lu_discovery_sources]	Contains the categories for all discovery sources.

Subscriptions form for the OTM products

Learn about the essential fields and indicators found on the Subscriptions form for our products, enabling streamlined subscription management and clarity in your OTM product usage.

View the following subscription statistics for items purchased individually (a la carte):

Name

The name of the OTM application.

Purchased

The number of purchased subscriptions per application.

Capacity Definition ID

The ID used for retrieving daily consumption data of subscription units from an application.

Start date/End date

The time duration during which this subscription remains active.

Subscriptions a la carte

The licensing module calculates and displays subscription consumption as follows:

Subscriptions a la carte

The Subscriptions window displays the information for purchased and allocated subscriptions for OTM applications.

Subscriptions window displaying subscriptions purchased a la carte

The screenshot shows a table with the following data:

Name	Start date	End date	Purchased	Allocated
Operational Technology Visibility - Subs...	2021-11-30	2024-11-29	25840	460

OTM Licensing dashboard

Use the OTM Licensing dashboard to assess resource consumption and status in relation to your acquired subscriptions. The dashboard provides dedicated reports for each OTM application, providing visual representations of daily usage counts and the average

utilization of subscription units over a 90-day period. The OTM Licensing dashboard is an integral component of ITOM Licensing application version 4.0, accessible at ServiceNow Store.

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](#).

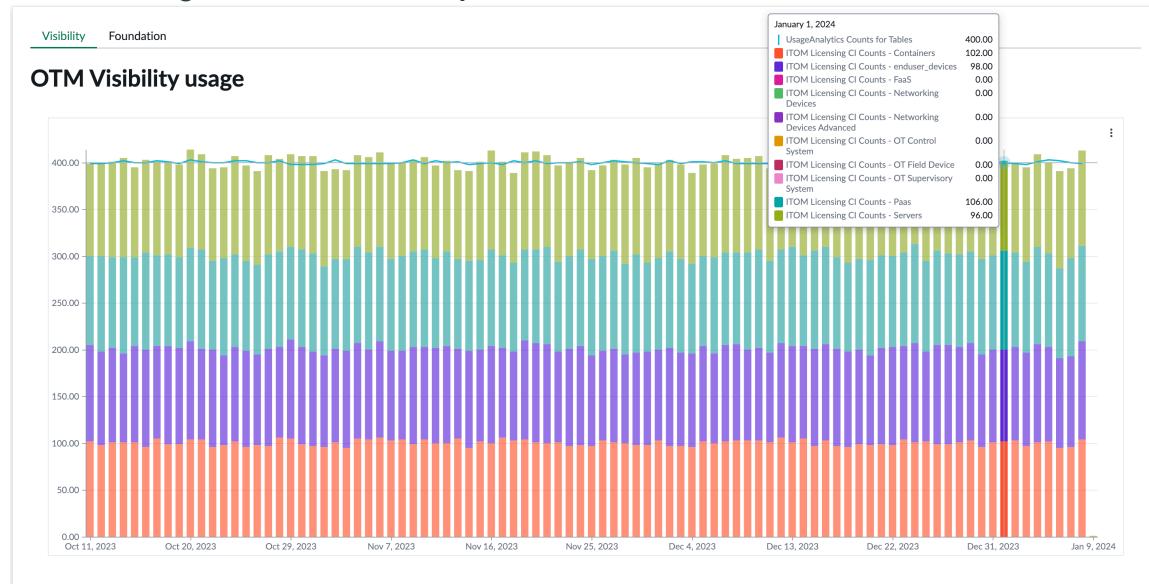
Required Now Platform roles

admin

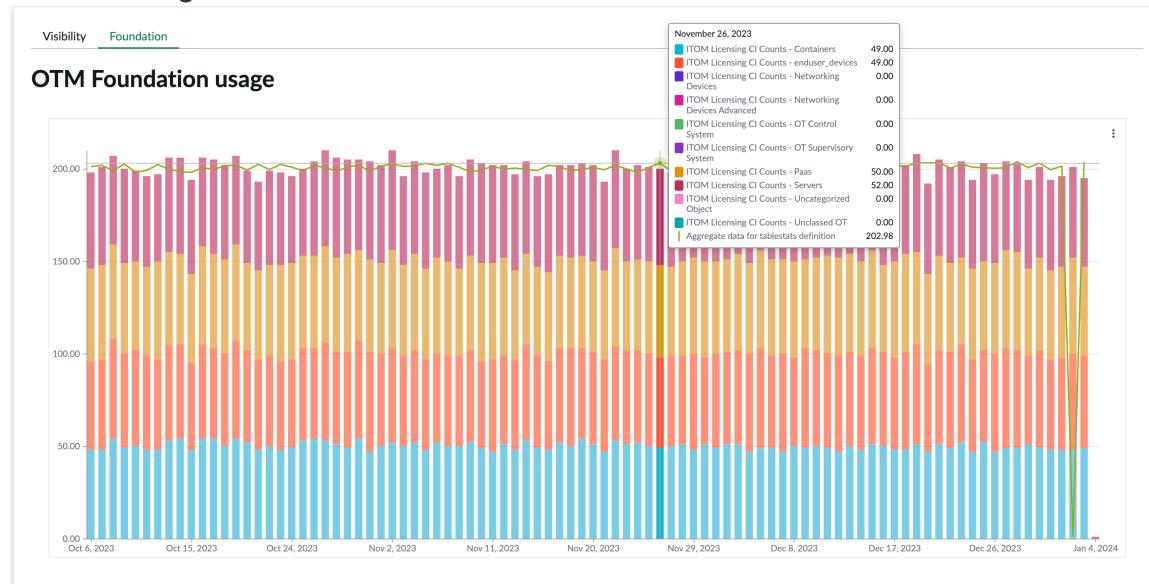
Access the Assessment dashboard

To open the dashboard for OTM, navigate to **All > OTM License > OTM Licensing Dashboard**.

OTM Licensing dashboard - Visibility



OTM Licensing dashboard - Foundation



Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

User	Dashboard use
admin	Validate the resource usage for different OTM products. Report the cases where the organization exceeded the number of purchased subscription units for specific resources.

Note: ServiceNow applications refer to devices and applications that comprise an application service as configuration items (CIs).

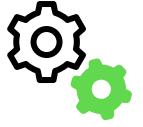
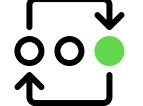
Data visualization

The dashboard includes the following visualization:

Title	Source table	Description
OTM Visibility Usage and OTM Foundation Usage	ITOM Licensing CI Counts [itom_lu_ci_counts] and UsageAnalytics Counts for Tables [usageanalytics_count]	<p>Displays bars that represent counts of CIs of different licensable categories for the last 120 days per ITOM application. The dashboard also displays the line that represents the average consumption of subscription units for the last 90 days.</p> <p>Note: CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days ago.</p>

Operational Technology Manager

The Operational Technology Manager application creates the foundational data and relationships that enable your organization to use the ServiceNow® Operational Technology solution. Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the Now Platform.

<p>Explore</p>  <p>Learn about how manufacturers use the Operational Technology Manager</p>	<p>Configure</p>  <p>Plan and configure your implementation</p>
<p>Use</p>  <p>Import, discover, and review Operational Technology devices</p>	<p>Integrate</p>  <p>Extend Operational Technology Manager by integrating it with other applications</p>
<p>Reference</p>  <p>Get details about related information and applications</p>	

Exploring the Operational Technology Manager

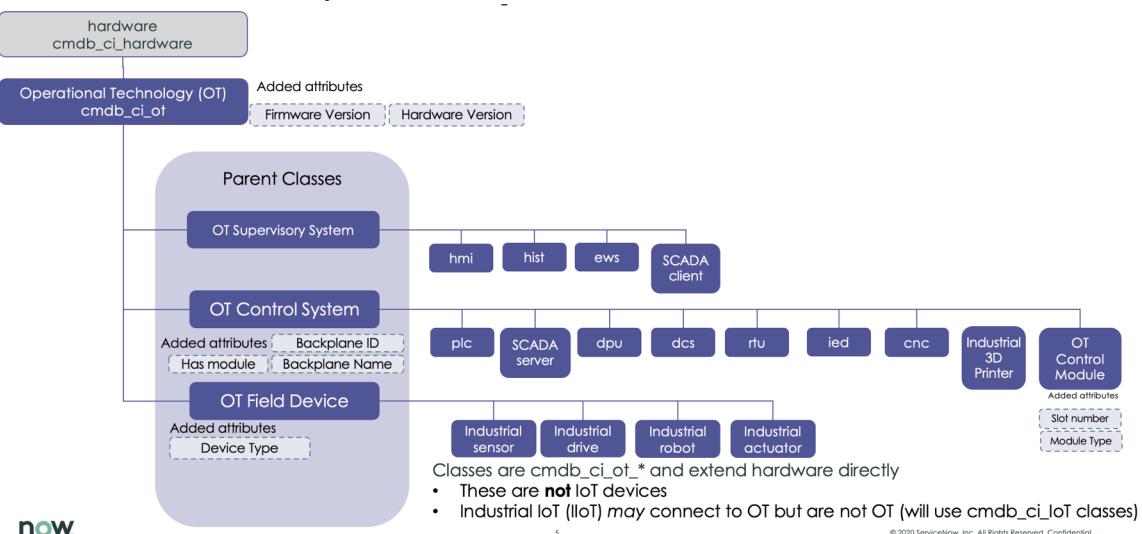
Learn how you can use the Operational Technology Manager application to create the foundational data and relationships that enable your enterprise to use the ServiceNow® Operational Technology solution.

The Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the Now Platform.

Operational Technology Manager (OT) configuration item extension classes

Operational Technology Manager uses Operational Technology (OT) configuration item (CI) extension classes that extend the CMDB class hierarchy as shown in the following figure.

OT CI extension classes equals OT devices



Operational Technology Manager includes class descriptions, identification rules, identifier entries, and dependent relationships, if applicable. The Service Graph applications use these class extensions to populate CIs and discover various technologies and software. To learn more, see [Operation Technology \(OT\) extension classes](#).

CMDB CI classes for Operational Technology Manager

Operational Technology Manager adds these Configuration Management Database (CMDB) configuration item (CI) classes that are part of the CMDB CI Class Models application.

Note: To learn more about this application, see the CMDB CI Class Models application in the [ServiceNow Store](#).

CMDB CI Classes for Operational Technology Manager Workflows

Class	Description	CI class extended
Network Intrusion Detection System	The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.	cmdb_ci_nids

OT device data import and discovery

Multiple methods are available for uploading your existing Operational Technology device data into the Now Platform.

Service Graph Connector (Excel)

You can use the Service Graph Connector (Excel) function to import your Operational Technology data from a populated Microsoft Excel flat-file spreadsheet. You use the spreadsheet in the Integration Hub Extract Transform Load (ETL) to upload this data to the CMDB. To learn more, see [Service Graph Connector for Operational Technology \(Excel\)](#).

Discovery for Operational Technology

To discover Operational Technology devices in designated Purdue levels in your Industrial Control System (ICS) networks, you run the Discovery for Operational Technology function on a recurring basis. It operates in a manner that is similar to the standard Discovery processes. However, its Discovery normally takes place in the Purdue levels 3 through 3.5, depending on which level you select when you create an OT discovery schedule. To learn more, see [Discovery for Operational Technology](#).

- Note:** To learn more about Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems.

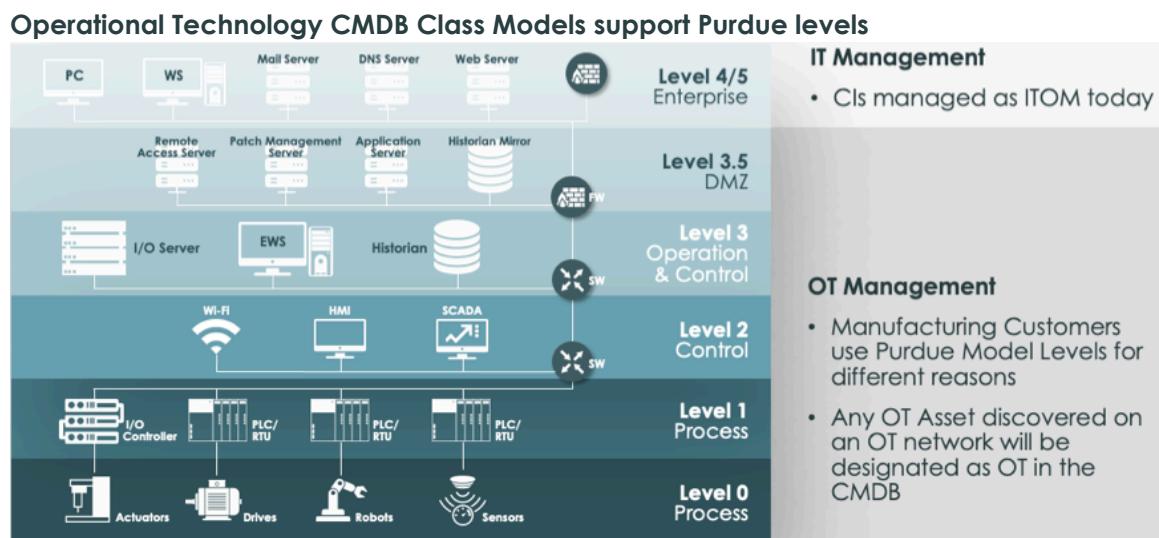
Service Graph Connectors from ServiceNow partners

ServiceNow partners also offer Service Graph Connectors that you can use to upload your existing OT data.

Differences between OT and standard IT networks

There are differences in how the Configuration Management Database (CMDB) handles the devices located in Operational Technology networks and those in standard Information Technology (IT) networks.

The following graphic depicts these differences:



Operational Technology Devices landing page tab

The Operational Technology (OT) Devices landing page tab is a centralized location in the Industrial Workspace that enables you to review your Operational Technology Manager and Industrial Process Manager data. You use it to review or edit detailed information for the OT devices and equipment model entities in your OT network.

The OT Devices landing page tab in the Industrial Workspace enables you to do the following actions:

- Understand what OT device information changed in your OT network in the past week.
- View the progress of an OT device inventory through an industrial facility.
- Analyze your OT devices in meaningful ways. For example, you can gain insights into how many of your production devices map to your production processes.

Note: The OT Devices landing page tab is included in the entitlement with the Operational Technology Manager application and runs in Performance Analytics. An additional license for Performance Analytics is not required. However, if you want to create new indicators, you need the Performance Analytics - Premium plugin. For more information, see [Activating your Performance Analytics subscription](#).

Landing page tab contents

To access OT device data in the OT Devices landing page tab, navigate to **All > Industrial Workspace**, select the Home () icon, and then select the **OT Devices** tab. To access the KPI graph for a tile, select the number count or chart component in the tile.

This table describes the OT device data that you see and can review in the OT Devices landing page tab.

OT Devices landing page tab

Tile	Description
Updates from the past 7 days	<p>Section that contains the counts for the critical changes related to OT devices that have occurred in your OT network the last seven calendar days.</p> <p>Note: If the job ran successfully, there's a Last updated: timestamp that indicates the end time of the last collection. If the job is unsuccessful, there's a Last executed timestamp that indicates the end time of the last execution.</p>
New OT devices discovered	Total number of new OT devices discovered by the Discovery for Operational Technology and other automated processes in your OT network during the last seven calendar days.
Inactive OT devices	Total number of OT devices that haven't appeared in your OT network during the last seven calendar days. These devices are considered inactive.
OT devices overview	<p>Section that contains the counts for the unclassified, unassigned, and unmapped OT devices.</p> <p>Note: If the job ran successfully, there's a Last updated: timestamp that indicates the end time of the last collection. If the job is unsuccessful, there's a Last executed timestamp that indicates the end time of the last execution.</p>

OT Devices landing page tab (continued)

Tile	Description
Unclassed	Total number of OT devices in your OT network that aren't assigned with an OT device type category.
Unassigned	Total number of OT devices in your OT network that aren't assigned to a user.
Unmapped	<p>Total number of OT devices in your OT network that aren't mapped to any site.</p> <p>i Note: This tile is only available when the Industrial Process Manager is installed because it requires the existence of an equipment model for mapping OT devices to a production process.</p>
OT devices by category	Section that contains the counts for the OT devices in your OT network, by their assigned OT device type classes.
Supervisory systems	Total number of OT devices in your OT network that are assigned to a Supervisory systems category.
Control systems	<p>Total number of OT devices in your OT network that are assigned to the Control systems category.</p> <p>i Note: Control modules are not included in this count.</p>
Field devices	Total number of OT devices in your OT network that are assigned to the Field devices category.
Computers and servers	Total number of OT devices in your OT network that are assigned to the Computers and servers category.
Network Gear	Total number of OT devices in your OT network that are assigned to the Network Gear category.
Industrial IoT	Total number of OT devices in your OT network that are assigned to the Industrial Internet of Things (IoT) category.
OT devices by Purdue level	Bar chart that indicates the total number of OT devices in your OT network by their assigned Purdue level.

OT Devices landing page tab (continued)

Tile	Description
	<p>Note: To learn more about Purdue levels in OT Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.</p>
OT devices by type (Top Level)	Bar chart that categorizes OT device data by OT device types.
OT devices by manufacturer (Top Level)	Pie chart that indicates the number of OT devices in your OT network by their assigned manufacturer.
OT devices by criticality	Pie chart that indicates the number of OT devices in your OT network by their assigned criticality.

OT landing page filters

The OT landing page offers filters to specify the data you see on your landing page at a per-site and business unit level.

Business unit filter

The business unit (BU) filter lets you do the following:

- View OT data for all business units.
- View OT data for a specific business unit.
- View OT data for multiple business units.

By default, the landing page shows OT data for all of your available BUs as shown in the following image.



To view OT data for one or more BUs, do these actions:

1. Select the **All business units** drop-down on the landing page header.
2. From the list, select one or more BUs that you want to see data for. You can use the search function to search for a specific BU.

Once you set the BU filter, the landing page displays data from every site included in the selected BUs. You can then choose a site from the **All Sites** drop-down, described in the next section. If you change the BU filter and select different BUs, the site filter is updated to only include sites associated with the new BU selection.

Site filter

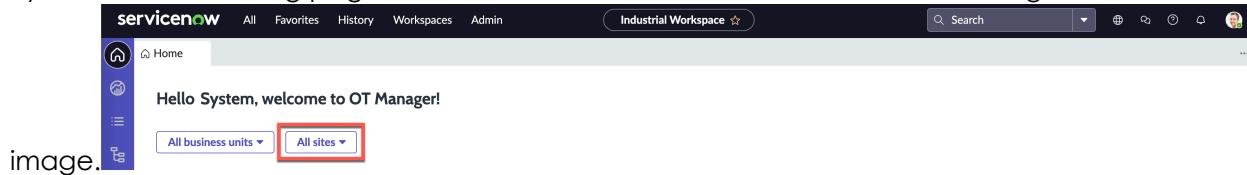
The site filter lets you do the following:

- View OT data for all sites.
- View OT data for a specific site.
- View OT data for multiple sites.
- View OT data for no site assigned.

Note: If there's no site assigned to an OT device, the filter shows **No site assigned**.

To have the correct sites shown on the landing page, you must assign a site to the device and then assign a business unit to that site.

By default, the landing page shows OT data for all sites as shown in the following



To view OT data for one or more sites, do these actions:

1. Select the **All sites** drop-down on the landing page header.
2. From the list, select one or more sites that you want to see data for.

Note: You can use the search function to search for a specific site. Type the name of the site or the short code in the search bar.

Setting up the OT Devices landing page tab

Complete the Guided Setup tasks to set up the OT Devices landing page tab with the correct data collections, indicator resources, and filters.

For more information about the OT Devices landing page tab and its contents, see [Operational Technology Devices landing page tab](#).

OT Devices landing page tab Guided Setup tasks

Task	Purpose
Complete the OT Devices Data Collection Configuration.	Collects and displays daily data for all indicators from Performance Analytics for the OT Devices landing page tab. You must complete this step before others can view the landing page tab.
[Optional] Review the indicator sources.	By default, each indicator of the OT Devices landing page tab can only show 1 million records. If you expect more than 1 million total records, you must override the records collection.
Create business units.	Create business units (BUs) to show BUs in the business unit filter for the OT Devices landing page tab.

OT Devices landing page tab Guided Setup tasks (continued)

Task	Purpose
	<p>Note: Only the BUs that are associated with sites are displayed in the landing page.</p>
Assign sites to business units	Assign sites to business units (BUs) to enable users to filter the landing page tabs by BU.

Configure the data collection for OT devices

Configure the data collection for Operational Technology (OT) devices to collect and display daily data for all indicators from Performance Analytics.

Before you begin

Role required: admin

About this task

When the OT Devices Daily Data Collection job hasn't run yet, no data is available for the landing page tab and the **Last updated** timestamp is hidden. If you're an admin, you see the following warning message that prompts you to run the OT Devices Daily Data Collection

job:

No Data is shown on the dashboard because the 'OT Devices Daily Data Collection' job has not been run yet. [Run job now](#)

Note: If you're not an admin, you see a warning message that prompts you to reach out to the admin for further assistance.

To run the OT Devices Daily Data Collection job, complete the following steps.

Procedure

1. Navigate to All > Data Collector > Performance Analytics > Jobs.

Alternatively, if you're in the OT Devices landing page tab, select **Run job now** in the error message.

2. Select the Show / hide filter () icon and apply a filter of [Name] [is] [OT Devices Daily Data Collection].

3. Select the check box next to the **Active** field under the **Job parameters** section and schedule a time in the **Time** field to start collecting data.

Alternatively, you can use the **Execute Now** button to collect data manually. Otherwise, no data is shown when you view the landing page tab. It's recommended to only use the **Execute Now** button when you first run the job. Everyday data collected after this point should be collected at a scheduled time.

4. Check if the default schedule collection time works for you.

The default time is 00:00:00 daily. If you want to change the default collection time, you can change it after activating the job. Please notify users of this change.

Result

The OT Devices landing page tab is now showing the correct data for the collected OT devices for your users.

Review the indicator sources for a larger number of records

Review the indicator sources if a larger number of records is needed, so that the landing page tab can show more records than the default value of 1 million and the error message is cleared.

Before you begin

Role required: admin

About this task

Due to the migration with Performance Analytics, each indicator of the OT Devices landing page tab can only show 1 million records by default. If you're an admin and records exceed 1 million after running the OT Devices Daily Data Collection job, you see the following error message that directs you to the job logs.

 The 'OT Devices Daily Data Collection' job ran with errors. Please review the job logs.

Note: If you're not an admin and the records exceed 1 million after running the OT Devices Daily Data Collection job, the error message directs you to the admin for help.

As an admin, you can check the job logs related list from link in the error message and filter out the information to see which indicator source has the error. After you find the indicator source with the error, you can change the indicator sources for a larger number of records. This helps ensure that the indicator source data can be overridden, an error message no longer appears for other users, and data is shown for the indicator source. For more information about indicator sources, see [Indicator sources](#).

Note: There may be warnings included in the job logs that aren't about the indicator sources. You must filter the job logs record by the **Level** column and find the error messages about indicator sources.

Procedure

1. Navigate to **All > Performance Analytics > Sources > Indicator Sources**.

2. Select the Show / hide filter () icon and apply the following filters.

- [Application] [is] [Operational Technology Manager]
- [Facts table] [is] [cmdb_ci]

After applying the filters, the table shows 6 device indicator

Name	Conditions	Facts table	Valid for frequency
Benchmark: Inactive OT Devices	OT device details is not empty.and. Mos...	Configuration Item [cmdb_ci]	Daily
Benchmark: Industrial IoT	OT device details is not empty.and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: New OT Devices Discovered	OT device details is not empty.and. Fir...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Computer and Servers	OT device details is not empty.and. Sys...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Devices	OT device details is not empty.and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Network Gear	OT device details is not empty.and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: Unmapped OT Devices	OT device details is not empty.and. Cre...	Configuration Item [cmdb_ci]	Daily

records.

3. Select the indicator source record that you need to change.

You can find which indicator source needs to be adjusted from job logs link in the error message.

4. In the Records Collection tab, select the check box next to the **Override records collection** field.

The **Maximum number of fetched records** field appears.

5. In the **Maximum number of fetched records** field, change the value to **xm**.

6. Select **Update**.

Create business units

Create business units (BUs) to enable the business unit filter for the OT Devices landing page tab.

Before you begin

Role required: admin

About this task

To show the business unit filter on the OT Devices landing page tab, the admin must create BUs to map to sites so that other users can see the BUs under the business unit filter on the OT Devices landing page tab.

Procedure

- 1.** Navigate to **All > Organization > Business Units**.
- 2.** Select **New**.
- 3.** On the form, fill in the following fields.

Business Unit form fields

Field	Description
Name	Name of the business unit.
Company	The company, if any, related with this business unit.
Business Unit Head	The person who heads the business unit.
Description	A description of the business unit.
Parent	Refers to another business unit. The Parent field makes the business unit as a hierarchy element.
Hierarchy level	A number or text to indicate the level of the business unit.
Related list	
Departments	Departments that comprise this business unit. Add as many departments as necessary.

4. Select **Submit**.

5. Optional: Repeat steps 2 through 4 as many times as needed until you create all your required BUs.

Result

The business unit is created. You can add a BU on a site record or in the Sites list.

Assign a site to a business unit

Assign a site to a business unit so that you can filter the landing page tab by business unit.

Before you begin

Role required: admin

About this task

You can assign a site to a business unit in the following ways.

- Editing the site record directly.
- Select multiple site records in the Sites table and update the Business Unit column.

Procedure

1. Navigate to **All > Equipment Model - ISA > Sites**.
2. To assign a site to a business unit by editing the site record, do these actions:
 - a. Select a site record to open it.
 - b. In the **Business Unit** field, add the appropriate business unit.
 - c. Select **Update**.
3. To select multiple site records in the Sites table and update the Business Unit column, do these actions:
 - a. In the Sites table, select the checkbox next to each site that you want to assign to a business unit.
 - b. In the **Business Unit** column, select the Column options button and choose **Update Selected**.
 - i Note:** The business unit column is only visible with the ISA Site view. If you don't see the Business Unit column, ensure that the Sites table view is set to **View: ISA Site**.
 - c. In the **Business Unit** field, add the business unit.
 - d. Select **Update**.

Configuring the Operational Technology Manager

Configure the Operational Technology Manager application so that you can create the data foundation for the ServiceNow® Operational Technology solution.

Task	Purpose
1. Install Operational Technology (OT) extension classes.	Extend the Configuration Management Database (CMDB) class hierarchy for use in Operational Technology processing.
2. Install Operational Technology Manager.	Install the Operational Technology Manager application.
3. Assign Operational Technology roles.	Assigns roles to control the actions that are available for each user.
4. Prepare a Microsoft Excel spreadsheet for Service Graph Connector import.	Create and populate a Microsoft Excel spreadsheet with your existing Operational Technology data for upload to the Now Platform.
5. Import your Excel spreadsheet.	Upload your Operational Technology data to the Configuration Management Database (CMDB).

Task	Purpose
6. Run the Discovery for Operational Technology function.	Discover Operational Technology (OT) devices in the designated Purdue levels in your Industrial Control System (ICS) networks.
7. Install Service Graph connectors that are provided by ServiceNow® partners.	Install ServiceNow, Inc. connectors that are provided by partners as they become available in the ServiceNow® Store.
8. Use the All OT Devices or All OT Devices by IP Address selections on the Operational Technology (OT) menu.	Edit or view detailed information for the OT devices in your enterprise, after you've imported your Excel spreadsheet, or have run the Discovery for Operational Technology function.

Operational Technology (OT) extension classes installation

You must install the Operational Technology (OT) extension classes that are the foundation of the Operational Technology Manager.

These class models extend the Configuration Management Database (CMDB) class hierarchy, which includes class descriptions, identification rules, identifier entries, and dependent relationships, if applicable. Applications, such as Discovery and Service Graph connectors, use these class extensions to populate CIs and discover various technologies and software.

To learn more, see [Operational Technology \(OT\) extension classes](#)

Install Operational Technology Manager

If you have the admin role, you can install the Operational Technology Manager application. The application includes demo data and installs that are related ServiceNow® Store applications and plugins, if they are not already installed.

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](#).

Note: To learn more about the subscriptions required for the Operational Technology Manager, see [Subscriptions for Operational Technology Management \(OTM\)](#)

Role required: admin

About this task

The following items are installed with Operational Technology Manager:

- Plugins
- Store applications
- Roles
- Tables
- Script includes

For more information on viewing components that are installed with an application, see [Find components installed with an application](#).

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Operational Technology Manager application 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 might 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.

Dependent plugins and applications appear if they will be installed, are currently installed, or must be installed. If any plugins or applications require installation, you must install them before you can install Operational Technology Manager.

4. Optional: If demo data is available and you want to install it, select the **Load demo data** check box.

Demo data comprises the sample records that describe application features for the common use cases. Load the 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**.

Script includes installed with Operational Technology Manager

The Operational Technology Manager plugin installs the following script includes.

Name	Description
BaseDAO	Base DAO class that all DAO classes should extend.
NIDSUtils	Utilities for the cmdb_ci_nids devices.
OTDevicesMigrationUtils	Migrate records from specified classes to updated class tables. For more information, see Operational Technology (OT) extension classes .
OTDevice	Implementation class for performing operations on the [cmdb_ot_entity] table and related [cmdb_ci] and [cmdb_rel_ci] tables.
OTDeviceDAO	Utilities to assist with using Discovery for Operational Technology devices.
OTBaseDAO	Base DAO class that all DAO classes in Operational Technology should extend.
OTFoundationConstants	A collection of constants used by other script includes.

Name	Description
OTUtils	A collection of Operational Technology utility methods.
SGOTDeviceConstants	A collection of constants used by Operational Technology service graph connectors.
SGOTDeviceTransformUtil	A collection of transform utility methods for Operational Technology service graph connectors.
SGOTDataStreamBase	Base pattern to invoke a specific data stream with given inputs.
SGOTTroubleShootHelper	Helper methods for validating the Service Graph Connector's configurations.
OTAssetFilterAjax	A utility client script to filter out application records and OT Control Modules from the All OT Devices list view in the Industrial Workspace.
OTBulkEditHandler	Server side script to handle the IT to OT bulk edit (conversion) and the OT device details bulk edit that are triggered through the Flow Actions and scheduled jobs.
Extension Points	
SGOTDeviceImportExtensionPoint	SG OT Device Import Extension Point which includes two methods: 1. getDeviceCMDBClassNameWithSysId; 2. getComputerType.

Assign Operational Technology Manager roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Operational Technology Manager application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the Operational Technology Manager application.

If you want to configure site users, you can create and assign user criteria for equipment model entity site users. For more information, see [Assign or remove equipment model site access for non-administrators](#).

Role	Description
Operational Technology Discovery Administrator [ot_discovery_admin]	Can run the Discovery for Operational Technology process, but cannot access the Configuration Management Database (CMDB) to view the configuration items (CIs) and related Operational Technology (OT) entities that are created from discovered

Role	Description
	items. To learn more, see Create an Operational Technology discovery schedule and run the Discovery process .
Operational Technology Manager Viewer [cmdb_ot_viewer]	Read-only access to Operational Technology (OT) device records.
Operational Technology Manager Editor [cmdb_ot_editor]	Create, read, update, and delete access for Operation Technology (OT) extension classes .
Operational Technology Manager Admin [cmdb_ot_admin]	Create, read, update, and delete access for Operational Technology (OT) device records. Can also edit and manage specific configurations in the OT entity type. To learn more, see Operation Technology (OT) extension classes .

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See User administration Assign a role Edit a role Delete a role Assign a role to a user Edit a user Delete a user
Assign a role to a group	See User administration Assign a role Edit a role Delete a role Assign a role to a group Edit a group Delete a group

Operational Technology Manager Integrations

The Operational Technology Manager application includes support for third-party integrations.

The following third-party integrations are currently supported.

- Service Graph Connector Integration for Claroty CTD
- Service Graph Connector for Microsoft Defender for IoT (Azure)
- Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

Service Graph Connector Integration for Claroty CTD

Integrate Claroty Continuous Threat Detection (CTD) with the ServiceNow Operational Technology Manager application to import detected devices and Claroty CTD sites (sensor or Network Intrusion Detection System appliances).

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](#).

Supported versions

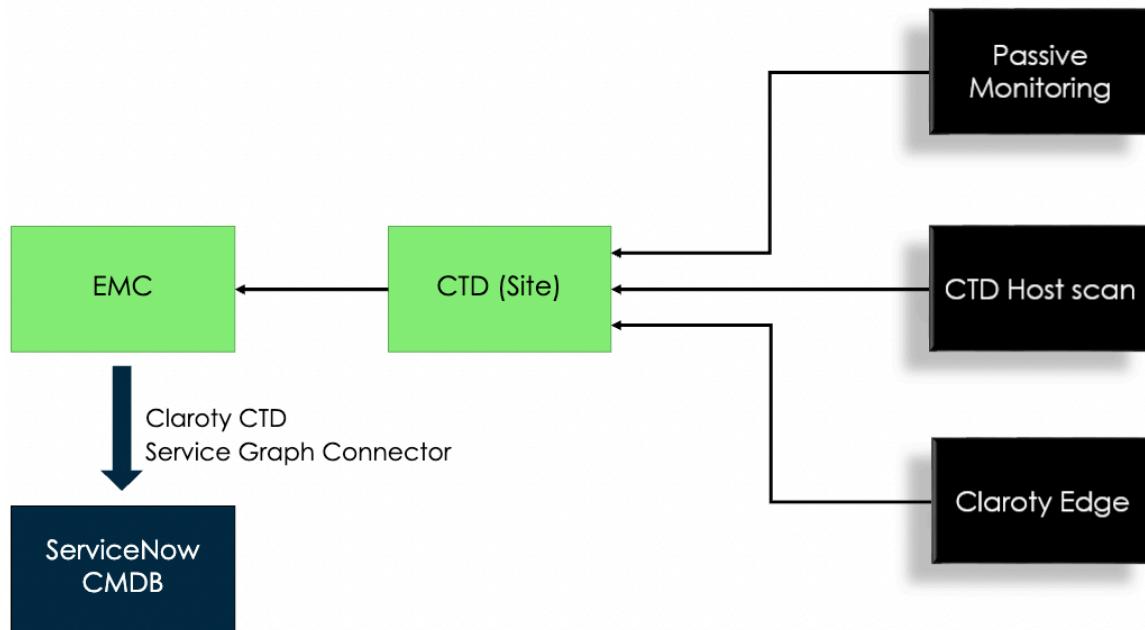
- Claroty CTD Version: 2.0.1 or later
- Supported ServiceNow Versions:
 - Utah
 - Vancouver
 - Washington

Use cases

Use the Service Graph Connector Integration for Claroty Continuous Threat Detection with the Operational Technology Manager application to import the following information to the Configuration Management Database (CMDB)

- Sites
- Devices detected by each site
- Connections (or baselines)
- Installed programs

The following figure shows the detection method for importing Claroty CTD data into the CMDB.



Guided setup

The guided setup for the Service Graph Connector Integration for Claroty CTD provides an organized sequence of tasks to configure the integration on your instance. To access the guided setup, see [Configure guided setup](#).

CMDB integrations dashboard

The Integration Commons for CMDB store app provides a dashboard with a central view of the status, processing results, and processing errors of all installed integrations. You can see metrics for all integration runs. You can filter the view to a specific CMDB integration, a specific time duration, or a specific integration run. For more details about monitoring

integrations in the CMDB Integrations Dashboard, see [Integration Commons for CMDB \(2.12.0\)](#).

Data mapping

Data from the Claroty CTD data sources is mapped and transformed into the ServiceNow CMDB Configuration Item (CI) class definitions using the Robust Transform Engine (RTE). Data is inserted into the ServiceNow CMDB using the Identification and Reconciliation Engine (IRE).

The following table lists the data sources included for the Service Graph Connector Integration for Claroty CTD and the corresponding staging tables where the imported data is loaded.

Data sources and staging tables for Claroty CTD

Data source	Staging table
SG-OT Claroty CTD Devices	SG-OT Claroty CTD Devices Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_devices_import]
SG-OT Claroty CTD Baselines	SG-OT Claroty CTD Baselines Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_baseline_import]
SG-OT Claroty CTD Programs	SG-OT Claroty CTD Programs Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_programs_import]
SG-OT Claroty CTD Sites	SG-OT Claroty CTD Sites Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_sites_import]

The imported data from the staging tables is then inserted into the following target tables:

- Computer [cmdb_ci_computer]
- Hardware [cmdb_ci_hardware]
- IP Address [cmdb_ci_ip_address]
- Network Adapter [cmdb_ci_network_adapter]
- OT Device Details [cmdb_ot_entity]
- OT Control Module [cmdb_ci_ot_control_module]
- OT Control System [cmdb_ci_ot_control]
- Serial Number [cmdb_serial_number]

For more information, see [CMDB classes targeted](#).

Default query parameters for the Service Graph Connector Integration for Claroty CTD

By default, the Service Graph Connector Integration for Claroty CTD is shipped with query parameter filters. You can modify their values based on ServiceNow entitlements that you have with the IntegrationHub Enterprise package.

When you begin importing the data from the Claroty CTD, the Service Graph Connector Integration for Claroty CTD uses the default query parameter filters that are listed in the following table.

Default query parameter filters

Query parameter filter	Value	Description
approved_exact	true	Unapproved devices on the Claroty CTD aren't imported because the value of approved_exact is set to true.
valid_exact	true	Invalid devices on the Claroty CTD aren't imported because the value of valid_exact is set to true.
special_hint_exact	0	Address types that aren't set to 0 (unicast) on the Claroty CTD aren't imported.
ghost_exact	false	If there's an device on the Claroty CTD that is classified as a ghost, the Service Graph Connector Integration for Claroty CTD doesn't import it because the default value is set to false.

Configure the Service Graph Connector Integration for Claroty CTD

Use the guided setup for Service Graph Connector Integration for Claroty CTD to lead you through the integration steps.

Before you begin

Dependencies and requirements:

- The [Integration Commons for CMDB \(2.12.0\)](#) ↗ store app, which is automatically installed.
- The [CMDB CI Class Models store app](#) ↗, which is automatically installed.
- The ITOM Discovery License plugin (com.snc.itom.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.itom.license). For more information, see [Request Discovery](#) ↗.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.

Role required: admin

Note: If you have an earlier version of the Service Graph Connector Integration for Claroty CTD, then don't migrate data from the old connector. You must uninstall the previous version and run the new integration.

Procedure

1. Ensure that the application is set to Service Graph Connector Integration for Claroty CTD by using the application picker.
For more information, see [Application picker](#) ↗.
2. Navigate to **All > Service Graph Connector Claroty CTD > Guided Setup**.

3. On the Getting started page, select **Get Started**.
4. To configure a MID Server, complete the following:
 - a. In the Setup Connections and Credentials section, select the Configure MID server task.
 - b. Select **Mark as complete** once you complete the MID Server configuration.
5. To set up the connections records, complete the following:
 - a. In the Setup Connections and Credentials section, select the Configure Connections task.
 - b. Select **Configure**.
 - c. Open the Claroty CTD API record in the Connections table.
 - d. In the **Connection URL** field, enter the name of the URL for your Claroty CTD Enterprise Management Console (EMC).
For example, <https://192.168.1.100>.
 - e. If you're using a MID Server, select the **Use MID Server** check box in the record.

Note: If you're not using a MID Server, go to step 5g.
 - f. From the Advanced MID Server Configuration related list, select a MID Server and a MID Selection.
 - g. Select **Update**.
 - h. Repeat steps 5a to 5h to update the **Claroty CTD EMC Base Auth** record.
6. To set up the credentials records, complete the following:
 - a. In the Setup Connections and Credentials section, select the Configure Credentials task.
 - b. Select **Configure**.
 - c. Open the Claroty CTD EMC Base Auth record in the Credentials table.
 - d. In the **User name** field, enter the user name that you used to log in to the Claroty CTD EMC.
 - e. In the **Password** field, enter the password that you used to log in to the Claroty CTD EMC.
 - f. Select **Update**.
7. To test the connection, complete the following:
 - a. In the Setup Connections and Credentials section, select the Test/Validate Connection task.
 - b. Select the **Test Connection** UI action from the related links section on the data source record for sensors.
After completing the connection test, view the results. You must perform the suggested troubleshooting steps until the test result returns **Success**.
 - c. Check that the connection manager has a valid certificate.

A valid certificate must be installed for a production environment. For a non-production or proof of concept (POC) instance, you can configure the system properties to enable the integration to work when the connection manager doesn't have a valid certificate. The following table lists the system properties that you can configure for a non-production environment.

System properties for a non-production environment

Property	Value
com.glide.communications.httpclient.verify	Set to false .
com.glide.communications.httpclient.verify_certificate	Set to false . If you need to add this system property, see Add a system property .
com.glide.communications.trustmanager_truststore	Set to true .

d. Check the MID security policy.

In the intranet record, verify that the columns in the following table show the specified values.

Intranet record values

Column	Value
Certificate chain check	false
Hostname check	false
Revocation check	false

For more information, see [MID Server certificate check policies](#).

8. To set the system properties that configure the API resource paths, pagination sizes, and API key expiration times, complete the following:

a. In the Configure System Properties section, select **Configure**.

b. Configure the system properties in the following table:

Property	Description
sn_clarotyctdsgc.resourcepath.site	<p>Property to set the resource path for the sites:</p> <p>i Note: The resource path for the sites is provided by default for the Claroty CTD Enterprise Management Console (EMC) V4.4.3 API version for the CTD sites and devices.</p> <p>If you want to use a different API version, you can override the paths.</p>

Property	Description
sn_clarotyctdsgc.resourcepath.device	<p>Property to set the resource path for the devices:</p> <p>i Note: The resource path for the devices is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices.</p> <p>If you want to use a different API version, you can override the paths.</p>
sn_clarotyctdsgc.pagesize.device	<p>Property to set the number of device records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page.</p> <p>i Note: 500 is the maximum number of devices per page.</p>
sn_clarotyctdsgc.resourcepath.baseline	<p>Property to set the resource path for the baselines:</p> <p>i Note: The resource path for the baselines is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices.</p> <p>If you want to use a different API version, you can override the paths.</p>
sn_clarotyctdsgc.pagesize.baseline	<p>Property to set the number of baseline records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page.</p>
sn_clarotyctdsgc.get_all_baselines	<p>Property to fetch all records for baselines or only the new records since the start time of the last successful import.</p> <p>i Note: When you import baselines for the first time, all records are imported regardless of the setting for this property.</p>
sn_clarotyctdsgc.resourcepath.entity	<p>Property to set the resource path for the entities:</p>

Property	Description
	<p>Note: The resource path for the entities is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices. If you want to use a different API version, you can override the paths.</p>
sn_clarotyctdsgc.resourcepath.program	<p>Property to set the resource path for the installed programs:</p> <p>Note: The resource path for the installed programs is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices.</p> <p>If you want to use a different API version, you can override the paths.</p>
sn_clarotyctdsgc.pagesize.entity	<p>Property to set the number of entity records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page.</p>
sn_clarotyctdsgc.pagesize.program	<p>Property to set the number of program records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page.</p>
sn_clarotyctdsgc.api_token_life_in_minutes	<p>Property to set the number of minutes that the API is considered active. After the time expires, the Service Graph Connector fetches a new API key during the next import. The default value is 0 and a new token is fetched for each REST call.</p> <p>Note: You can change the value to keep the same token for a maximum of 24 hours and reduce the number of REST calls.</p>
sn_clarotyctdsgc.classify_based_on_os	<p>Property to provide a list of classes that support the classification by OS as part of the Service Graph Connector Integration for Claroty CTD.</p> <p>When the flag is set to True, the classification by OS is supported. When it is set to False, the Service Graph Connector no longer classifies by OS. For example:</p>

Property	Description
	<pre data-bbox="843 164 1287 227">{ "cmdb_ci_ip_switch":true, "cmdb_ci_nids":false }</pre>
sn_clarotyctdsgc.filter.asset_type_code	<p>Property to provide a list of codes for device types separated by the delimiter (\$).</p> <p>For more information about Claroty types and codes, see CMDB classes targeted. For example, to only import PLC and HMI device types, enter the Claroty type code as 0\$1.</p>
sn_clarotyctdsgc.filter.asset_purdue_level	<p>Property to provide a list of Purdue Levels separated by the delimiter (\$). For example, to only filter devices with Purdue Levels 1 and 2, To only filter Devices with Purdue Level 1 & 2, set the value as 1.0\$2.0.</p>

- c. Select **Save**.
9. To import CTD sites, complete the following:
- In the Configure CTD Sites section, select the Import CTD Sites task.
 - Select **Configure**.
 - Select the **Execute Now** button.
10. To configure Network Intrusion Detection Systems (NIDS), complete the following:
- In the Configure CTD Sites section, select the Configure NIDS task.
 - Select **Mark as Complete** once you setup the NIDS used to get devices from Claroty CTD.
11. To configure the import schedules to run the sites, devices, baselines, and installed programs, complete the following:
- In the Configure Import Schedules section, select the Configure Sites Import Schedule task.
 - Select **Configure**.
 - In the Scheduled Data Imports table, select **SG-OT CTD Sites Scheduled Import**.
 - By default, the sites import schedule is configured to run every day at midnight.
 - You must import and validate the CTD sites before you import the devices.
 - Complete the following actions as needed to review or change the import schedule as needed:

Action	Description
Enter a conditional script	Enter a conditional script that determines whether a scheduled import should run by selecting Conditional .
Change the default import schedule	Change the default import schedule by setting the Run field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the Runs as field. i Note: By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see Configure guided setup .
Activate the import	Activate the import by selecting the Active check box.
Save any schedule changes	Save any schedule changes by selecting Update .

- e. In the Configure Import Schedules section, select the Configure Devices Import Schedule task.
- f. Select **Configure**.
- g. In the Scheduled Data Imports table, select **SG-OT CTD Devices Scheduled Import** to review or change the import schedule for your devices.
 - By default, the devices import schedule is configured to run every day at midnight.
 - Devices are queried by the CTD site. The Service Graph Connector only queries for devices that are detected by validated CTD sites.
- h. Complete the following actions as needed to review or change the import schedule as needed:

Action	Description
Enter a conditional script	Enter a conditional script that determines whether a scheduled import should run by selecting Conditional .

Action	Description
Change the default import schedule	Change the default import schedule by setting the Run field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the Runs as field. i Note: By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see Configure guided setup .
Activate the import	Activate the import by selecting the Active check box.
Save any schedule changes	Save any schedule changes by selecting Update .

- i. In the Configure Import Schedules section, select the Configure Baselines Import Schedule task.
- j. Select **Configure**.
- k. In the Scheduled Data Imports table, select **SG-OT CTD Baselines Scheduled Import** to review or change the import schedule for the baselines.
By default, the baselines import schedule is configured to run after the parent OT Control System runs.
- l. Complete the following actions as needed to review or change the import schedule as needed.

Action	Description
Enter a conditional script	Enter a conditional script that determines whether a scheduled import should run by selecting Conditional .
Change the default import schedule	Change the default import schedule by setting the Run field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the Runs as field.

Action	Description
	<p>Note: By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.</p>
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see Configure guided setup .
Activate the import	Activate the import by selecting the Active check box.
Save any schedule changes	Save any schedule changes by selecting Update .

- m. In the Configure Import Schedules section, select the Configure Sites Installed Programs Import Schedule task.
- n. Select **Configure**.
- o. In the Scheduled Data Imports table, select **SG-OT CTD Installed Programs Scheduled Import** to review or change the schedule for the installed programs import. By default, the installed programs import schedule is configured to run every day at midnight.
- p. Complete the following actions as needed to review or change the import schedule as needed.

Action	Description
Enter a conditional script	Change the default import schedule by setting the Run field as necessary.
Change the default import schedule	Change the default import schedule by setting the Run field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the Runs as field.
	<p>Note: By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.</p>
Run an import	Run an import by selecting Execute Now. You can import either all records or only

Action	Description
	new records since the start time of the last successful import, based on the system properties configured. For more information, see step 7c.
Activate the import	Activate the import by selecting the Active check box.
Save any schedule changes	Save any schedule changes by selecting Update .

12. Optional: To troubleshoot the Service Graph Connector Integration for Claroty CTD, complete the following:
- Select the [OPTIONAL] Troubleshooting the Service Graph Connector for Claroty CTD section.
 - In the Execute the validations scheduled job task, select **Configure**.
 - Select **Execute Now**.
This job performs tasks to validate the configurations for SGC and the connection to Claroty CTD. If configuration issues are found, the validation results report the problem and suggest troubleshooting steps. Wait for the scheduled job to finish.
 - Once the scheduled job is complete, navigate back to the [OPTIONAL] Troubleshooting the Service Graph Connector for Claroty CTD section.
 - In the Review validation results task, select **Configure**.
This step opens the execution logs and suggestions of the last troubleshooting run for you to view.
 - Address the suggestions as needed.

Note: You can use the scheduled script at any point after the initial configuration of the Service Graph Connector Integration for Claroty CTD. To trigger validations, navigate to **All > Service Graph Connector for Claroty CTD > Troubleshooting > Run Troubleshooting**. To view the validation results, navigate to **All > Service Graph Connector for Claroty CTD > Troubleshooting > Results**.

For additional information about troubleshooting issues while using the Service Graph Connector Integration for Claroty CTD, see [Troubleshooting scenarios for the Service Graph Connector Integration for Claroty CTD \(KB1502041\)](#).

Validate NIDS sensors

Validate the Network IDS (NIDS) sensors once they're imported to prepare for device import. The sensors can only pass the validation if they aren't in learning mode as such sensors aren't eligible for device import.

Before you begin

It's recommended that you have the CSDM plugin installed. The Service Graph Connector aligns with the life cycle data models as per the CMDB standards. For more information, see [Implementing the CSDM framework in stages](#).

Role required: cmdb_nids_admin

About this task

The **Life Cycle Stage** and **Life Cycle Stage Status** fields are used to capture the learning mode of a sensor. If the Life Cycle Stage field is set to **Operational** and Life Cycle Stage Status is set to **Learning Mode**, then validation is unsuccessful. If the Life Cycle Stage Status field is set to **In Use**, the validation is successful.

Procedure

1. Navigate to **All > Network IDS Appliances (NIDS) > Sensors**.
2. Select the sensor record that you want to validate.
3. In the NIDS Assigned Meta Data section, add values for the sensor that you want to be assigned to the detected devices.
4. In the NIDS Admin Configuration section, make sure that the **Life Cycle Stage Status** field value isn't **Learning Mode**. Otherwise, the validation fails.
5. Make sure that the **NIDS network type** field is set based on the NIDS network location. For example, you can select an NIDS network type of **IT** for a data center deployment of the NIDS, or an NIDS network type of **OT** for an industrial deployment on an Industrial/OT network.
If you select OT, the OT device details are created for all devices.
6. When the attributes are correctly filled out, select **Validate**.

Note:

NOTE: The attributes passed from the sensor to the devices are defined in the `sn_cmdb_ci_class.nids_map_fields` system property. The following list is the default list of attributes.

- assigned_to
- location
- company
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- zone
- isa_entity_site (only available if you have the Industrial Process Manager application installed)

Use the Service Graph Connection framework

Use the Service Graph Connection framework to gather the related data sources, system properties, and scheduled data imports created for Claroty CTD in one place.

Before you begin

Role required: admin

About this task

There are application modules available to navigate to the data sources, system properties, and scheduled data imports for the Service Graph Connector Integration for Clarity CTD separately. However, the new Service Graph Connection framework makes it possible to gather all the related data sources and scheduled data imports created for Clarity CTD in one place. You can also test the connection to the source (Clarity CTD) using the related links section.

Procedure

1. Ensure that the application scope is set to the **Service Graph Connector Integration for Clarity CTD** application by using the application picker.
2. Navigate to **All > Service Graph Connector for Clarity CTD > Clarity CTD SGC Connection**.
3. On the Service Graph Connections page, select **SG-OT Clarity CTD Default Connection**.
4. Optional: To access the system properties, select the **Service Graph Connection Properties** tab.
5. Optional: To access the data sources, select the **Service Graph Connection Data Sources** tab.
6. Optional: To access the scheduled data imports, select the **Service Graph Connection Scheduled Data Imports** tab.
7. Optional: To test your connection with the Clarity CTD platform, select the **Test Connection** related link.

You can test your connection at any time. When the connection test is complete, you can find the status and suggestions for troubleshooting the failed steps under **Status** and **Suggestion** on the same page respectively.

CMDB classes targeted in the Service Graph Connector Integration for Clarity CTD

When you complete the setup tasks, you can configure the integration periodically to pull data from Clarity CTD. The data is saved in tables that extend from the Configuration item [cmdb_ci] table.

Computer [cmdb_ci_computer]

The following attributes in the Computer [cmdb_ci_computer] table are populated by collected data:

Attribute label	Attribute name
Last discovered	last_discovered
Firmware version	firmware_version
OS version	os, os_version

Hardware [cmdb_ci_hardware]

The following attributes in the Hardware [cmdb_ci_hardware] table are populated by collected data:

Attribute label	Attribute name
Device class name	device_class_name

Attribute label	Attribute name
First seen	first_seen
Last seen	last_seen
First discovered	first_discovered
Serial number	serial_number
Model number	model_number
Manufacturer	manufacturer
Vendor	vendor

IP Address [cmdb_ci_ip_address]

The following attributes in the IP Address [cmdb_ci_ip_address] table are populated by collected data:

Attribute label	Attribute name
IP address	ip_address
IP version	ip_version

Network Adapter [cmdb_ci_network_adapter]

The following attributes in the Network Adapter [cmdb_ci_network_adapter] table are populated by collected data:

Attribute label	Attribute name
MAC address	mac_address

OT Device Details [cmdb_ot_entity]

The following attributes in the OT Device Details [cmdb_ot_entity] table are populated by collected data:

Attribute label	Attribute name
OT device type	ot_device_type
Business criticality	business_criticality
OT correlation ID	ot_correlation_id
Purdue level	purdue_level
Zone	zone

OT Control Module [cmdb_ci_ot_control_module]

The following attributes in the OT Control Module [cmdb_ci_ot_control_module] table are populated by collected data:

Attribute label	Attribute name
Slot	slot
Name	name
Firmware version	firmware_version
Model	model
Serial number	serial_number
Manufacturer	manufacturer
Vendor	vendor

OT Control System [cmdb_ci_ot_control]

The following attributes in the OT Control System [cmdb_ci_ot_control] table are populated by collected data:

Attribute label	Attribute name
Last discovered	last_discovered

Serial Number [cmdb_serial_number]

The following attributes in the Serial Number [cmdb_serial_number] table are populated by collected data:

Attribute label	Attribute name
Serial number	serial_number

Default class mapping

A default class mapping is shipped with the Service Graph Connector Integration for Claroty CTD application.

Note: You can find the class mapping in the `sn_clarotyctdsgc.SGOTClarotyCTDConstants` script.

Claroty CTD Type	ServiceNow Type	Class	OT Entity Type	Claroty Types and Codes
eAAAServer	(Empty)	cmdb_ci_server		eAAAServer = 61
eAccessControl	(Empty)	cmdb_ci_iot		eAccessControl = 50
eAccessPoint	(Empty)	cmdb_ci_ip_switch		eAccessPoint = 60
eADServer	(Empty)	cmdb_ci_server		eADServer = 33
eAutonomousVehicle	(Empty)	cmdb_ci_ot_field_device	device	eAutonomousVehicle = 58

Clarity CTD Type	ServiceNow Type	Class	OT Entity Type	Clarity Types and Codes
eAVServer	(Empty)	cmdb_ci_server		eAVServer = 32
eBarcodeScanner	OT Field Device	cmdb_ci_ot_field_device		eBarcodeScanner = 48
eBluetoothDevice	(Empty)	cmdb_ci_iot		eBluetoothDevice = 41
eBroadcast	(Empty)	cmdb_ci_netgear		eBroadcast = 4
eCamera	OT Field Device	cmdb_ci_ot_field_device		eCamera = 42
eCleaningDevice	OT Field Device	cmdb_ci_ot_field_device		eCleaningDevice = 55
eController	OT Control System	cmdb_ci_ot_control_system		eController = 20
eDataLogger	OT Control System	cmdb_ci_ot_control_system		eDataLogger = 66
eDBServer	(Empty)	cmdb_ci_server		eDBServer = 35
eDomainController	(Empty)	cmdb_ci_server		eDomainController = 5
eElectricalDrive	Industrial Drive	cmdb_ci_ot_industrial_drive		eElectricalDrive = 68
eEndpoint	Operational Technology Device	cmdb_ci_ot	ot_base	eEndpoint = 2
eEngineeringStation	EWS	cmdb_ci_ot_ews	ews	eEngineeringStation = 14
eFileServer	(Empty)	cmdb_ci_server		eFileServer = 10
eFirewall	(Empty)	cmdb_ci_ip_firewall		eFirewall = 31
eFrontEndProcessor	OT Control System	cmdb_ci_ot_control_system		eFrontEndProcessor = 26
eGateway	(Empty)	cmdb_ci_ip_switch		eGateway = 15
eGPSClock	Operational Technology Device	cmdb_ci_ot	ot_base	eGPSClock = 37
eGPSDevice	Operational Technology Device	cmdb_ci_ot	ot_base	eGPSDevice = 62
eHistorian	Historian	cmdb_ci_ot_historian	historian	eHistorian = 9
eHMI	HMI	cmdb_ci_ot_hmi	hmi	eHMI = 1
eHomeAssistant	(Empty)	cmdb_ci_iot		eHomeAssistant = 53
eIED	IED	cmdb_ci_ot_ied	ied	eIED = 19
eInfusionPump	(Empty)	cmdb_ci_iot		eInfusionPump = 46

Clarity CTD Type	ServiceNow Type	Class	OT Entity Type	Clarity Types and Codes
eMediaServer	(Empty)	cmdb_ci_server		eMediaServer = 54
eMedicalDevice	(Empty)	cmdb_ci_iot		eMedicalDevice = 47
eMicroscope	(Empty)	cmdb_ci_iot		eMicroscope = 49
eModem	(Empty)	cmdb_ci_netgear		eModem = 27
eMotorStarter	Industrial Drive	cmdb_ci_ot_industrial_drive		eMotorStarter = 69
eNetworkAccessStorage	(Empty)	cmdb_ci_server		eNetworkAccessStorage = 30
eNetworking	(Empty)	cmdb_ci_netgear		eNetworking = 3
eNTPServer	(Empty)	cmdb_ci_server		eNTPServer = 21
eOPCServer	OPC Server	cmdb_ci_ot_opc_server		eOPCServer = 16
eOT	Operational Technology Device	cmdb_ci_ot	ot_base	eOT = 17
ePLC	PLC	cmdb_ci_ot_plc	plc	ePLC = 0
ePrinter	(Empty)	cmdb_ci_printer		ePrinter = 6
eProxyServer	(Empty)	cmdb_ci_netgear		eProxyServer = 28
eRemoteIO	OT Field Device	cmdb_ci_ot_field_device	device	eRemoteIO = 13
eReverseProxyServer	(Empty)	cmdb_ci_netgear		eReverseProxyServer = 29
eRobot	Industrial Robot	cmdb_ci_ot_industrial_robot	robot	eRobot = 57
eRouter	Router	cmdb_ci_ip_router		eRouter = 11
eRTU	RTU	cmdb_ci_ot_rtu	rtu	eRTU = 18
eSCADAClient	SCADA Client	cmdb_ci_ot_scadaclient	client	eSCADAClient = 7
eSCADAMaster	SCADA Server	cmdb_ci_ot_scadams	server	eSCADAMaster = 38
eSCADAServer	SCADA Server	cmdb_ci_ot_scadaserver	server	eSCADAServer = 8
eSensor	Industrial Sensor	cmdb_ci_ot_industriesensor	sensor	eSensor = 67
eSmartLight	(Empty)	cmdb_ci_iot		eSmartLight = 51
eSmartPhone	(Empty)	cmdb_ci_iot		eSmartPhone = 44
eSmartWatch	(Empty)	cmdb_ci_iot		eSmartWatch = 45

Clarity CTD Type	ServiceNow Type	Class	OT Entity Type	Clarity Types and Codes
eStorageArray	(Empty)	cmdb_ci_server		eStorageArray = 36
eStreamer	(Empty)	cmdb_ci_iot		eStreamer = 52
eSwitch	(Empty)	cmdb_ci_ip_switch		eSwitch = 12
eSyslogServer	(Empty)	cmdb_ci_server		eSyslogServer = 25
eTerminalServer	(Empty)	cmdb_ci_server		eTerminalServer = 24
eTVScreen	(Empty)	cmdb_ci_iot		eTVScreen = 40
eUPS	(Empty)	cmdb_ci_ups		eUPS = 63
eUserConsole	HMI	cmdb_ci_ot_hmi	hmi	eUserConsole = 22
eUserWorkstation	HMI	cmdb_ci_ot_hmi	hmi	eUserWorkstation = 23
eVendingMachine	(Empty)	cmdb_ci_iot		eVendingMachine = 43
eVideoRecorder	(Empty)	cmdb_ci_server		eVideoRecorder = 64
eVirtualizationServer	(Empty)	cmdb_ci_server		eVirtualizationServer = 65
eVoipPhone	(Empty)	cmdb_ci_comm_hardware		eVoipPhone = 39
eVoipServer	(Empty)	cmdb_ci_server		eVoipServer = 56
eWebServer	(Empty)	cmdb_ci_server		eWebServer = 34
eWirelessLanController	(Empty)	cmdb_ci_netgear		eWirelessLanController = 59
eBarcodeReader	(Empty)	cmdb_ci_iot		eBarcodeReader = 77
eBiometricScanner	(Empty)	cmdb_ci_iot		eBiometricScanner = 74
eDNSServer	(Empty)	cmdb_ci_server		eDNSServer = 75
eSNMPScanner	(Empty)	cmdb_ci_server		eSNMPScanner = 73
eSNMPServer	(Empty)	cmdb_ci_server		eSNMPServer = 72
eVisionCamera	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eVisionCamera = 76
eVisionController	OT Control System	cmdb_ci_ot_control_system	ot_control_system	eVisionController = 78
eVisionSensor	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eVisionSensor = 79

Clarity CTD Type	ServiceNow Type	Class	OT Entity Type	Clarity Types and Codes
eVOIPAccessPoint (Empty)		cmdb_ci_ip_switch		eVOIPAccessPoint = 71
eVulnerabilityScanner (Empty)		cmdb_ci_server		eVulnerabilityScanner = 70

Service Graph Connector for Microsoft Defender for IoT (Azure)

Integrate Microsoft Defender for IoT with the ServiceNow® Operational Technology Manager application to automate import of OT devices and sensor appliances.

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](#).

Supported versions

- Supports Microsoft Defender for IoT sensor versions:
 - 22.2.3.22
 - 22.2.5.9
- Supported ServiceNow versions:
 - Utah
 - Vancouver
 - Washington

Use cases

You can use the Service Graph Connector for Microsoft Defender for IoT (Azure) with the ServiceNow® Operational Technology Manager application to import OT devices and sensor appliances.

Guided setup

The guided setup for the Service Graph Connector for Microsoft Defender for IoT (Azure) provides an organized sequence of tasks to configure the integration on your instance. To access the guided setup, see [Configure guided setup](#).

CMDB integrations dashboard

The Integration Commons for CMDB store app provides a dashboard with a central view of the status, processing results, and processing errors of all installed integrations. You can see metrics for all integration runs. You can filter the view to a specific CMDB integration, a specific time duration, or a specific integration run. For more details about monitoring integrations in the CMDB Integrations Dashboard, see [Integration Commons for CMDB \(2.12.0\)](#).

Data mapping

Data from the Microsoft Defender for IoT (Azure) data sources is mapped and transformed into the ServiceNow CMDB Configuration Item (CI) class definitions using the Robust

Transform Engine (RTE). Data is inserted into the ServiceNow CMDB using the Identification and Reconciliation Engine (IRE).

When you complete the setup, you can configure the integration to periodically pull data from the Microsoft Defender for IoT (Azure) application.

The following table lists the data sources included for a Microsoft Defender for IoT (Azure) project and the corresponding staging tables where the imported data is loaded.

Data sources and staging tables for Microsoft Defender for IoT (Azure)

Data source	Staging table
SG-OT Azure D4IoT Devices Import	SG-OT Azure D4IoT Devices Import [sn_msftd4iotazsgc_sg_ot_azure_d4iot_devices_import]
SG-OT Azure D4IoT Sensors Import	SG-OT Msft D4IoT Sensors Import [sn_msftd4iotazsgc_sg_ot_azure_d4iot_sensors_import]

The imported data from the staging tables is then inserted into the following target tables:

- AIX Server [cmdb_ci_aix_server]
- Computer [cmdb_ci_computer]
- Configuration Item [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX Server [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- External System Metadata [cmdb_key_value_v2]
- Game Console [cmdb_ci_game_console]
- Handheld Computing Device [cmdb_ci_handheld_computing]
- Historian [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX Server [cmdb_ci_hpx_server]
- HVAC Equipment [cmdb_ci_hvac]
- HyperV Server [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- Industrial Actuator [cmdb_ci_ot_industrial_actuator]
- Industrial Drive [cmdb_ci_ot_industrial_drive]
- Industrial Robot [cmdb_ci_ot_industrial_robot]
- Industrial Sensor [cmdb_ci_ot_industrial_sensor]
- IoT Device [cmdb_ci_iot]
- IP Address [cmdb_ci_ip_address]
- IP Camera [cmdb_ci_ip_camera]
- IP Firewall [cmdb_ci_ip_firewall]
- IP Phone [cmdb_ci_ip_phone]
- Linux Server [cmdb_ci_linux_server]

- Netgear [cmdb_ci_netgear]
- Network Adapter [cmdb_ci_network_adapter]
- Network Intrusion Detection System [cmdb_ci_nids]
- Operational Technology (OT) [cmdb_ci_ot]
- OSX Server [cmdb_ci_osx_server]
- OT Control Module [cmdb_ci_ot_control_module]
- OT Control System [cmdb_ci_ot_control]
- OT Device Details [cmdb_ot_entity]
- OT Field Device [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- Printer [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- Serial Number [cmdb_serial_number]
- Server [cmdb_ci_server]
- Server [cmdb_ci_server]
- Solaris Server [cmdb_ci_solaris_server]
- Source [sys_object_source]
- Unix Server [cmdb_ci_unix_server]
- Uninterruptible Power Supply (UPS) [cmdb_ci_ups]
- Wireless Access Point [cmdb_ci_wap_network]

For more information on where data is saved when pulling data from a Microsoft Defender for IoT (Azure) project, see [CMDB classes targeted](#).

Configure the Service Graph Connector for Microsoft Defender for IoT (Azure)

Use the guided setup for the Service Graph Connector for Microsoft Defender for IoT (Azure) to lead you through the integration steps.

Before you begin

Dependencies and requirements:

- The [Integration Commons for CMDB \(2.12.0\)](#) ↗ store app, which is automatically installed.
- The [CMDB CI Class Models store app](#) ↗, which is automatically installed.
- The ITOM Discovery License plugin (com.snc.item.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.item.license). For more information, see [Request Discovery](#) ↗.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.

Role required: admin

Note: If you have an earlier version of the Service Graph Connector for Microsoft Defender for IoT (Azure), then don't migrate data from the old connector. You must uninstall the previous version and run the new integration.

Procedure

1. Ensure that the application scope is set to the Service Graph Connector for Microsoft Defender for IoT (Azure) application by using the application picker.
For more information, see [Application picker ↗](#).
2. Navigate to **All > Service Graph for MSFT D4IoT (Azure) > Guided Setup**.
3. On the Getting started page, select **Get Started**.
4. To access the Azure resources, complete the following:
 - a. Select the Access to Azure Resources task.
 - b. Once you complete the instructions in the description, select **Mark as Complete**.
5. To set up the connections and credentials, complete the following:
 - a. In the Configure Connections and Credentials section, select the Setup Connections and Credentials task.
 - b. Select **Configure**.
 - c. Select the **SG-OT Azure Connection** record.
 - d. Select the Create New Connection & Credential related link.
 - e. In the Create Connection and Credential window, fill in the following fields.

Field	Description
Connection Name	Display name for the connection record
Connection URL	Azure URL
OAuth Client ID	Client ID (application ID) or Service Principal ID
OAuth Client Secret	Client secret key associated with the Service Principal
OAuth Token URL	URL to fetch Authorization token. Replace <tenantid> in the URL with the Tenant ID value.

i Note: When a token generation is successful, a new window appears with a success message. When a token generation isn't successful, a new window with the error message `OAuth flow failed` appears. Please check the details provided and try again by editing the record you created.

- f. Select **Create and Get OAuth Token**.
6. To test the connection, complete the following:

a. In the Setup Connections and Credentials section, select the Test/Validate Connection task.

b. Select the **Test Connection** UI action from the related links section on the data source record for sensors.

After completing the connection test, view the results. You must perform the suggested troubleshooting steps until the test result returns **Success**.

7. To configure the system properties, complete the following:

a. In the Configure System Properties section, select **Configure**.

b. Configure the following system properties.

Property	Description
sn_msftd4iotazsgc.resource_path	<p>Set the resource path property.</p> <p>The default Resource Path for the ARG REST API version 2021-03-01 is /providers/Microsoft.ResourceGraph/resources.</p>
sn_msftd4iotazsgc.pagesize.sensor	<p>Set the page size property for sensors.</p> <ul style="list-style-type: none"> ▪ As Azure ARG REST API supports pagination, you can choose the number of records per page for each API. ▪ The default is 1000 records per page. <p>i Note: 1000 is also the maximum number of records per page.</p>
sn_msftd4iotazsgc.pagesize.device	<p>Set the page size property for devices.</p> <ul style="list-style-type: none"> ▪ As Azure ARG REST API supports pagination, you can choose the number of records per page for each API. ▪ The default is 1000 records per page. <p>i Note: 1000 is also the maximum number of records per page.</p>
sn_msftd4iotazsgc.get_all_devices	<ul style="list-style-type: none"> ▪ For devices, you can choose to fetch all records (box checked) or the delta (box unchecked). ▪ The DELTA fetches all the records created or updated since the start time of the last successful import in the CMDB. <p>i Note: When you run the Devices Integration for the first time, all records are imported independent of this property.</p>

Property	Description
sn_msftd4iotazsgc.convert_sensor_names_to_lowercase	<p>Set this property for devices import.</p> <ul style="list-style-type: none"> This system property is used to convert the sensor names provided by Microsoft Azure into lowercase while importing devices. This is required as Microsoft Azure expects data for the query in a lowercase format.
sn_msftd4iotazsgc.filter.device_sub_types	<p>Set this property for filtering the devices during device import by sub type.</p> <ul style="list-style-type: none"> Comma-separated list of Microsoft Azure sub types to filter the devices. For example: to import only PLCs and servers, provide the value from the DeviceSubType attribute from Microsoft Azure as Server, PLC.
sn_msftd4iotazsgc.filter.device_tags	<p>Set this property for filtering the devices during device import by device tag.</p> <ul style="list-style-type: none"> Comma-separated list of case sensitive tags that are needed to filter devices. For example: to import devices with specific tags, provide a list of values from the DeviceTags attribute in Microsoft Azure.
sn_msftd4iotazsgc.filter.custom_query	<p>Set this property to add more filters for device import apart from the Device SubType and Device Tags filter.</p> <ul style="list-style-type: none"> Query to filter based on other attributes. This allows filtering for other attributes. For more information, see Azure Query Language.

c. Select **Save**.

8. To import sensors, complete the following:

a. In the Configure Sensors (NIDS) section, select the Import Sensors task.

b. Select **Configure**.

c. Select **Active** to activate the Scheduled Data Import job.

9. To configure the NIDS, complete the following:

a. In the Configure Sensors (NIDS) section, select the Import Sensors task.

b. Select **Mark as complete** once you complete the NIDS configuration linked in the description.

10. To configure import schedules, complete the following:

- a. In the Configure Import Schedules section, select **Configure**.
- b. Select **SG-OT Microsoft Azure D4IoT Sensors Scheduled Import** to review or change the sensors import schedule as needed.
 - i. Select **Active** to activate the sensors import schedule.
 - ii. By default, the sensors import schedule is configured to run daily at midnight. Change the schedule using the **Run** and **Time** fields.
 - iii. Select the **Conditional** check box to make this schedule conditional.
 - iv. Select **Execute Now** to start a manual import.
- c. Select **SG-OT Microsoft Azure D4IoT Devices Scheduled Import** to review or change the devices import schedule as needed.
 - i. Select **Active** to activate the sensors import schedule.
 - ii. By default, the sensors import schedule is configured to run daily at midnight. Change the schedule using the **Run** and **Time** fields.
 - iii. Select the **Conditional** check box to make this schedule conditional.
 - iv. Select **Execute Now** to start a manual import.

Note: Devices are queried per sensor. The Service Graph Connector only queries for devices detected by a validated sensor. For more information, see step 9.

11. Optional: To troubleshoot the Service Graph Connector for Microsoft Defender for IoT (Azure), complete the following:
 - a. Select the [OPTIONAL] Troubleshooting the Service Graph Connector for Microsoft Defender for IoT (Azure) section.
 - b. In the Execute the validations scheduled job task, select **Configure**.
 - c. Select **Execute Now**.
This job performs tasks to validate the configurations for SGC and the connection to Microsoft Azure. If configuration issues are found, the validation results report the problem and suggest troubleshooting steps. Wait for the scheduled job to finish.
 - d. Once the scheduled job is complete, Navigate back to the [OPTIONAL] Troubleshooting the Service Graph Connector for Microsoft Defender for IoT (Azure) section.
 - e. In the Review validation results task, select **Configure**.
This step opens the execution logs and suggestions of the last troubleshooting run for you to view.
 - f. Address the suggestions as needed.
- Note:** You can use the scheduled script at any point after the initial configuration of the Service Graph Connector Integration for Clarity CTD. To trigger validations, navigate to **All > Service Graph for MSFT D4IoT (Azure) > Troubleshooting > Run Troubleshooting**. To view the validation results, navigate to **All > Service Graph for MSFT D4IoT (Azure) > Troubleshooting > Results**.

What to do next

You can now connect Microsoft Defender for IoT (Azure) with the ServiceNow Service Graph Connector for Microsoft Defender for IoT (Azure). For more information, see [Connecting your Microsoft Defender for IoT \(Azure\) subscription to the ServiceNow Service Graph Connector for Microsoft Defender for IoT \(Azure\) \(KB1587770\)](#).

Validate NIDS sensors

Validate the Network IDS (NIDS) sensors once they're imported to prepare for the device import. Sensors only pass the validation if they aren't in learning mode as such sensors are not eligible for device import.

Before you begin

It's recommended that you have the CSDM plugin installed. The Service Graph Connector aligns with the life cycle data models as per the CMDB standards. For more information, see [Implementing the CSDM framework in stages](#).

Role required: cmdb_nids_admin

Note: An NIDS appliance in ServiceNow represents a Microsoft Defender for IoT (Azure) sensor.

About this task

The **Life Cycle Stage** and **Life Cycle Stage Status** fields are used to capture the learning mode of a sensor. If the Life Cycle Stage field is set to **Operational** and Life Cycle Stage Status is set to **Learning Mode**, then validation is unsuccessful. If the Life Cycle Stage Status field is set to **In Use**, the validation is successful.

Procedure

1. Navigate to **All > Network IDS Appliances (NIDS) > Sensors**.
2. Select the sensor record that you want to validate.
3. In the NIDS Assigned Meta Data section, add values for the sensor that you want to be assigned to the detected devices.
4. From the NIDS Admin Configuration section, make sure that the **Life Cycle Stage Status** field value isn't **Learning Mode**.
Otherwise, the validation fails.
5. Make sure that the **NIDS network type** field is set based on the NIDS network location.
For example, you can select an NIDS network type of **IT** for a data center deployment of the NIDS, or an NIDS network type of **OT** for an industrial deployment on an Industrial/OT network.

If you select OT, the OT device details are created for all devices.

- When the attributes are correctly filled out, select **Validate**.

 Note:

NOTE: The attributes passed from the sensor to the devices are defined in the `sn_cmdb_ci_class.nids_map_fields` system property. The following list is the default list of attributes.

- assigned_to
- location
- company
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- zone
- isa_entity_site (only available if you have the Industrial Process Manager application installed)

Use the Service Graph Connection framework

Use the Service Graph Connection framework to gather the related data sources, system properties, and scheduled data imports created for Microsoft Azure in one place.

Before you begin

Role required: admin

About this task

There are application modules available to navigate to the data sources, system properties, and scheduled data imports for the Service Graph Connector for Microsoft Defender for IoT (Azure) separately. However, the new Service Graph Connection framework makes it possible to gather all the related data sources and scheduled data imports created for Microsoft Azure in one place. You can also test the connection to the source (Microsoft Azure) using the related links section.

Procedure

- Ensure that the application scope is set to the Service Graph Connector for Microsoft Defender for IoT (Azure) application by using the application picker.
- Navigate to **All > Service Graph for MSFT D4IoT (Azure) > Azure SGC Connection**.
- On the Service Graph Connections page, select **SG-OT Azure SGC Default Connection** record.
- Optional: To access the system properties, select the **Service Graph Connection Properties** tab.
- Optional: To access the data sources, select the **Service Graph Connection Data Sources** tab.

6. Optional: To access the scheduled data imports, select the **Service Graph Connection Scheduled Data Imports** tab.

7. Optional: To test your connection with the Microsoft Azure platform, select the **Test Connection** related link.

You can test your connection at any time. When the connection test is complete, you can find the status and suggestions for troubleshooting the failed steps under **Status** and **Suggestion** on the same page respectively.

CMDB classes targeted in the Service Graph Connector for Microsoft Defender for IoT (Azure)

When you complete the guided setup, you can configure the integration to periodically pull data from a Microsoft Defender for IoT (Azure) project. The data is saved in tables that extend from the Configuration item [cmdb_ci] table.

Computer [cmdb_ci_computer]

The following attributes in the Computer [cmdb_ci_computer] table are populated by collected data:

Attribute label	Attribute name
Operation system	os
OS version	os_version
OS domain	os_domain
OS address width	os_address_width

Configuration Item [cmdb_ci]

The following attributes in the Configuration Item [cmdb_ci] table are populated by collected data:

Attribute label	Attribute name
Hardware vendor	manufacturer
Most recent discovery	most_recent_discovery
First discovered	first_discovered
Name	name
Display name	sys_class_name

IP Address [cmdb_ci_ip_address]

The following attributes in the IP Address [cmdb_ci_ip_address] table are populated by collected data:

Attribute label	Attribute name
IP Address	ip_address

Network Adapter [cmdb_ci_network_adapter]

The following attributes in the Network Adapter [cmdb_ci_network_adapter] table are populated by collected data:

Attribute label	Attribute name
MAC address	name, mac, mac_address

OT Control Module [cmdb_ci_ot_control_module]

The following attributes in the OT Control Module [cmdb_ci_ot_control_module] table are populated by collected data:

Attribute label	Attribute name
Firmware version	firmware_version
Model ID	model_id
Rack number	rack_number
Serial number	serial_number
Vendor	vendor
Most recent discovery	most_recent_discovery
First discovered	first_discovered

OT Device Details [cmdb_ot_entity]

The following attributes in the OT Device Details [cmdb_ot_entity] table are populated by collected data:

Attribute label	Attribute name
Purdue level	purdue_level
Asset criticality	asset_criticality

PLC [cmdb_ci_ot_plc]

The following attributes in the PLC [cmdb_ci_ot_plc] table are populated by collected data:

Attribute label	Attribute name
Switch position	switch_position
Switch remote mode	switch_remote_mode

Attribute mapping and classification for Service Graph Connector for Microsoft Defender for IoT (Azure)

The following tables describe the attribute mapping and classification for sensors and devices.

Sensors attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	<ul style="list-style-type: none"> sys_object_source cmdb_ci_nids 	<ul style="list-style-type: none"> snk in sys_object_source correlation_id 	Unique ID for the sensor.
name	String	cmdb_ci_nids	name	Name of the sensor.
properties.hostname	String	cmdb_ci_nids	fqdn	Host name of the sensor.
properties.ip	String	cmdb_ci_ip_address	ip_address	IP address of the sensor.
properties.learningMode	Boolean	cmdb_ci_nids	<p>False or unavailable:</p> <p>Life Cycle Stage (life_cycle_stage) : Operational</p> <p>Life Cycle Stage Status (life_cycle_stage_status) : In Use</p> <p>True:</p> <p>Life Cycle Stage (life_cycle_stage) : Operational</p> <p>Life Cycle Stage Status (life_cycle_stage_status) : Learning</p>	Learning mode status of the IoT sensor.
properties.mac	String	cmdb_ci_network_interface	mac_address	MAC address of the sensor.
properties.sensorStatus	String	cmdb_ci_nids	connection_state	Status of the IoT sensor.
properties.sensorVersion	String	cmdb_ci_nids	firmware_version	Version of the IoT sensor.
properties.upSince	Date and time as string	cmdb_ci_nids	first_discovered	Startup time.
properties.zone	String	cmdb_ci_nids	zone	Zone of the IoT sensor.

Devices attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/subscription-id>/providers/<providers-id>/location/<location>/deviceGroups/<device-Group>/devices/<name-field>	<ul style="list-style-type: none"> sys_object_source cmdb_ot_entity cmdb_key_value 	<ul style="list-style-type: none"> snk in sys_object_source • discovery_source_id in cmdb_ot_entity 	Unique ID for the device.
resourceGroup	(Empty)	cmdb_key_value	(Empty)	Resource group
tenantId	(Empty)	cmdb_key_value	(Empty)	Tenant ID
properties.authorizedState	String	cmdb_key_value	(Empty)	Authorized state of the device
properties.criticality	String	cmdb_ot_entity	business_criticality	Criticality of the device
properties.deviceName	String	cmdb_ci	name	Name of the device.
properties.deviceSubType	String	cmdb_ci	sys_class_name	Device subtype display name.
properties.firstSeenDate	Date and time as string	<ul style="list-style-type: none"> cmdb_ci cmdb_ci_ot_control_module (if control modules are present) 	first_discovered	First time the device was seen.
properties.lastSeenDate	Date and time as string	<ul style="list-style-type: none"> cmdb_ci cmdb_ci_ot_control_module (if control modules are present) 	most_recent_discovery	Everytime the device was seen.
properties.purdueLevel	String	cmdb_ot_entity	purdue_level	Purdue level of the device.
properties.operatingSystem	System distribution	cmdb_ci_computers	os	OS distribution
properties.operatingSystemVersion	System version	cmdb_ci_computers	os_version	OS version
properties.operatingSystemPlatform	System platform	cmdb_ci_computers	os_domain	OS platform
properties.operatingSystemArchitecture	System architecture	cmdb_ci_computers	os_address_width	OS architecture
properties.additionalFields.plcKeyState	(Empty)	cmdb_ci_ot_plc	switch_position	PLC key state

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.additionalFields.plcRunState	(Empty)	cmdb_ci_ot_plc	switch_remote_mode	PLC run state
properties.hardwareObject	(Empty)	(Empty)	(Empty)	Device hardware data
properties.hardwareString	String	cmdb_ci	(Empty)	Hardware model
properties.hardwareString	String	cmdb_serial_number	serial_number	Hardware serial number
properties.hardwareString	String	cmdb_ci	manufacturer	Hardware vendor
properties.nics	Array of Objects	(Empty)	(Empty)	List of the device network interface cards.
properties.nics[{}]	Object	(Empty)	(Empty)	Network interface card properties
properties.nics[{}].ipAddress	String	cmdb_ci_ip_address	ip_address	IPv4 address
properties.nics[{}].macAddress	String	cmdb_ci_network_interface	mac_address	MAC Address
properties.slots	Array of Objects	(Empty)	(Empty)	List of the device slot in the backplane.
properties.slots[{}]	Object	(Empty)	(Empty)	Slot data in PLC backplane.
properties.slots[{}].firmwareVersion	String	cmdb_ci_ot_controllermodule	firmware_version	Firmware version of the slot.
properties.slots[{}].model	String	cmdb_ci_ot_controllermodule	model	Model of the slot.
properties.slots[{}].rackNumber	Integer	cmdb_ci_ot_controllermodule	rack_number	Rack number in the backplane
properties.slots[{}].serialNumber	String	cmdb_ci_ot_controllermodule	serial_number	Serial number of the slot.
properties.slots[{}].slotNumber	Integer	cmdb_ci_ot_controllermodule	slot_number	Slot number inside the rack.
properties.slots[{}].hardwareVendor	String	cmdb_ci_ot_controllermodule	hardware_vendor	Hardware vendor of the slot.

Device type classification

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Alarm Siren	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Alarm System	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
ATM	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Backup Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Barcode Scanner	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DB Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
DCS Controller	Industrial	(Empty)	DCS	cmdb_ci_ot_dcs	NULL
Domain Controller	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Door Control Panel	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DVR	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Elevator	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Engineering Station	Industrial	(Empty)	EWS	cmdb_ci_ot_ews	EWS
Fire Alarm	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Fire Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Firewall	(Empty)	(Empty)	IP Firewall	cmdb_ci_ip_firewall	NULL
Game console	(Empty)	(Empty)	Game Console	cmdb_ci_game_console	NULL
Historian	(Empty)	(Empty)	Historian	cmdb_ci_ot_historian	Historian
HMI	Industrial	(Empty)	HMI	cmdb_ci_ot_hmi	HMI
Humidity Sensor	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
HVAC	(Empty)	(Empty)	HVAC Equipment	cmdb_ci_hvac	NULL
I/O Adapter	(Empty)	(Empty)	Network Adapter	(Empty)	NA
IED	(Empty)	(Empty)	IED	cmdb_ci_ot_ied	ied
Industrial Packaging System	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Industrial Robot	(Empty)	(Empty)	Industrial Robot	cmdb_ci_ot_industrial_robot	Industrial Robot
Industrial Scale	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Intercom	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
IP Camera	(Empty)	(Empty)	IP Camera	cmdb_ci_ip_camera	NULL
IP Telephone	(Empty)	(Empty)	IP phone	cmdb_ci_ip_phone	NULL
Marquee	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Meter	(Empty)	(Empty)	Industrial Sensor	cmdb_ci_ot_industrial_sensor	Industrial Sensor
Motion Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Multicast/Broadcast	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
NTP Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
People Counter System	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Physical Location	(Empty)	(Empty)	(Empty)	(Empty)	NULL
PLC	Industrial	(Empty)	PLC	cmdb_ci_ot_plc	PLC
Pneumatic Device	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Printer	(Empty)	(Empty)	Printer	cmdb_ci_printer	NULL
Protocol Converter	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Punch Clock	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Robot Controller	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
Router	(Empty)	(Empty)	IP Router	cmdb_ci_ip_router	NULL
RTU	(Empty)	(Empty)	RTU	cmdb_ci_ot_rtu	NULL
Server	Server	(Empty)	Server	cmdb_ci_server	NULL
Servo Drive	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Slot	(Empty)	(Empty)	OT Control Module	cmdb_ci_ot_control_module	OT Control Module
Smart Light	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart Phone	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Smart Switch	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Smart TV	(Empty)	(Empty)	Smart Television	cmdb_ci_stv	NULL
Storage	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Switch	Network Device	(Empty)	IP Switch	cmdb_ci_ip_switch	NULL
Tablet	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Terminal Station	(Empty)	(Empty)	Computer	cmdb_ci_computer	NULL
Thermostat	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Turnstile	(Empty)	(Empty)	IoT device	cmdb_ci_iot	
Uninterruptable Power Supply	(Empty)	(Empty)	UPS	cmdb_ci_ups	NULL
Variable Frequency Drive	(Empty)	(Empty)	Industrial Drive	cmdb_ci_ot_industrial_drive	Industrial Drive
VPN Gateway	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wifi Pineapple	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wireless Access Point	(Empty)	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL
WLAN access point	Network Device	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL
Workstation	Workstation	(Empty)	Computer	cmdb_ci_computer	NULL
Unknown	All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Unclassified	Unclassified or All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any other type	(Empty)	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • windows server • windows server, 	Windows Server	cmdb_ci_linux_server	Same as when the operating system isn't present.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
		<ul style="list-style-type: none"> version 2004[8] • windows server, version 1909[9] • windows server, version 1903[9] • windows server 2019 • windows server 2016 • windows server 2012 r2 • windows server 2012 • windows server 2008 r2 • windows server 2008 • windows server 2003 r2 • windows server 2003 • windows 2000 server • windows nt 4.0 server • windows nt 3.51 server • windows nt 3.5 server • windows nt 3.1 server 			
Any above type value except with	(Empty)	<ul style="list-style-type: none"> • linux • arch 	Linux Server	cmdb_ci_linux_server	Same as when the operating

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
designation Network and IoT		<ul style="list-style-type: none"> • centos • debian • fedora • suse • red hat • rhel • ubuntu • oracle 			system isn't present.
Any above type value except with designation Network and IoT	(Empty)	aix	AIX Server	cmdb_ci_aix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	esx	ESX Server	cmdb_ci_esx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • hp/ux • hpx 	HP-UX Server	cmdb_ci_hpx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • hyper-v • hyperv • hyper 	Hyperv Server	cmdb_ci_hyper_v_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • solaris • sunos • sun os 	Solaris Server	cmdb_ci_solaris_server	Same as when the operating system isn't present.
Any above type value except with designation	(Empty)	<ul style="list-style-type: none"> • macos x server • macos server 	OSX Server	cmdb_ci_osx_server	Same as when the operating system isn't present.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Network and IoT		<ul style="list-style-type: none"> • OS X • OSX 			
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • unix • gnu 	Unix Server	cmdb_ci_unix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • win • windows • Microsoft • windows 1.0, 1.02, 1.03, 1.04, 2.03, 2.10, 2.11, 3.0, 3.1, 3.2, 7, 8, 8.1, 10, 98, 95 • windows 2000 • windows for workgroups 3.11 • windows me • windows nt 3.1, 3.5, 3.51, 4.0 • windows vista • windows xp • windows xp professional x64 edition 	Base Computer class	cmdb_ci_computer	Same as when the operating system isn't present.
Any above type value except with designation	(Empty)	server	Base Server Class	cmdb_ci_server	Same as when the operating system isn't present.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Network and IoT					

Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

Integrate Microsoft Defender for IoT (On-premises Management Console) with the ServiceNow® Operational Technology Manager application to automate import of sensor appliances, OT devices, and network connections.

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](#).

Supported versions

- Microsoft Defender for IoT (On-premises Management Console) version: 10.5.2# or later
- Supported ServiceNow versions:
 - Utah
 - Vancouver
 - Washington

Use cases

You can use the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) with the ServiceNow® Operational Technology Manager application to import sensor appliances, OT devices, and network connections.

Guided setup

The guided setup for the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) provides an organized sequence of tasks to configure the integration on your instance. To access the guided setup, see [Configure guided setup](#).

CMDB integrations dashboard

The Integration Commons for CMDB store app provides a dashboard with a central view of the status, processing results, and processing errors of all installed integrations. You can see metrics for all integration runs. You can filter the view to a specific CMDB integration, a specific time duration, or a specific integration run. For more details about monitoring integrations in the CMDB Integrations Dashboard, see [Integration Commons for CMDB \(2.12.0\)](#).

Data mapping

Data from the Microsoft Defender for IoT (On-premises Management Console) data sources is mapped and transformed into the ServiceNow CMDB Configuration Item (CI) class

definitions using the Robust Transform Engine (RTE). Data is inserted into the ServiceNow CMDB using the Identification and Reconciliation Engine (IRE).

When you complete the setup, you can configure the integration to periodically pull data from the Microsoft Defender for IoT (On-premises Management Console) application.

The following table lists the data sources included for a Microsoft Defender for IoT (On-premises Management Console) project and the corresponding staging tables where the imported data is loaded.

Data sources and staging tables for Microsoft Defender for IoT (On-premises Management Console)

Data source	Staging table
SG-OT Microsoft D4IoT Connections Import	SG-OT Msft D4IoT Connections Import [sn_msftd4iotsgc_sg_ot_msft_d4iot_connections_import]
SG-OT Microsoft D4IoT Devices Import	SG-OT Msft D4IoT Devices Import [sn_msftd4iotsgc_sg_ot_msft_d4iot_devices_import]
SG-OT Microsoft D4IoT Sensors Import	SG-OT Msft D4IoT Sensors Import [sn_msftd4iotsgc_sg_ot_msft_d4iot_sensors_import]

The imported data from the staging tables is then inserted into the following target tables:

- AIX Server [cmdb_ci_aix_server]
- Computer [cmdb_ci_computer]
- Configuration Item [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX Server [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- External System Metadata [cmdb_key_value_v2]
- Game Console [cmdb_ci_game_console]
- Handheld Computing Device [cmdb_ci_handheld_computing]
- Historian [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX Server [cmdb_ci_hpxu_server]
- HVAC Equipment [cmdb_ci_hvac]
- HyperV Server [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- Industrial Actuator [cmdb_ci_ot_industrial_actuator]
- Industrial Drive [cmdb_ci_ot_industrial_drive]
- Industrial Robot [cmdb_ci_ot_industrial_robot]
- Industrial Sensor [cmdb_ci_ot_industrial_sensor]
- IoT Device [cmdb_ci_iot]
- IP Address [cmdb_ci_ip_address]
- IP Camera [cmdb_ci_ip_camera]

- IP Firewall [cmdb_ci_ip_firewall]
- IP Phone [cmdb_ci_ip_phone]
- Linux Server [cmdb_ci_linux_server]
- Netgear [cmdb_ci_netgear]
- Network Adapter [cmdb_ci_network_adapter]
- Network Intrusion Detection System [cmdb_ci_nids]
- Operational Technology (OT) [cmdb_ci_ot]
- OSX Server [cmdb_ci_osx_server]
- OT Control Module [cmdb_ci_ot_control_module]
- OT Control System [cmdb_ci_ot_control]
- OT Device Details [cmdb_ci_ot_entity]
- OT Field Device [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- Printer [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- Serial Number [cmdb_serial_number]
- Server [cmdb_ci_server]
- Server [cmdb_ci_server]
- Solaris Server [cmdb_ci_solaris_server]
- Source [sys_object_source]
- Unix Server [cmdb_ci_unix_server]
- Uninterruptible Power Supply (UPS) [cmdb_ci_ups]
- Wireless Access Point [cmdb_ci_wap_network]

For more information on where data is saved when pulling data from a Microsoft Defender for IoT (On-premises Management Console) project, see [CMDB classes targeted](#).

Configure the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

Use the guided setup for the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) to lead you through the integration steps.

Before you begin

Dependencies and requirements:

- The [Integration Commons for CMDB \(2.12.0\)](#) ↗ store app, which is automatically installed.
- The [CMDB CI Class Models store app](#) ↗, which is automatically installed.
- The ITOM Discovery License plugin (com.snc.itom.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.itom.license). For more information, see [Request Discovery](#) ↗.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.

Role required: admin

- Note:** If you have an earlier version of the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console), then don't migrate data from the old connector. You must uninstall the previous version and run the new integration.

Procedure

1. Ensure that the application scope is set to the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) application by using the application picker.
For more information, see [Application picker](#).
2. Navigate to **All > Service Graph Connector Microsoft D4IoT > Guided Setup**.
3. On the Getting started page, select **Get Started**.
4. To configure a MID Server, complete the following:
 - a. In the Setup Connections and Credentials section, select the Configure MID server task.
 - b. Select **Mark as complete** once you complete the MID Server configuration linked in the description.
5. To update the Connection and Credentials Alias record, complete the following:
 - a. In the Setup Connections and Credentials section, select the Connections and Credentials task.
 - b. Select **Configure**.
 - c. Open the default record **Microsoft D4IoT Base API**.
 - d. From the Connections related list, select **New** to create a new HTTP(s) Connection record.
 - e. In the **Connection URL** field, enter the name for the URL of your Microsoft Defender for IoT Central Manager.
For example, `https://192.168.1.100`.
 - f. Optional: If you are using a MID Server, select all of the following:
 - **Use MID Server** box
 - **MID Server** from the Advanced MID Server Configuration related list
 - **MID Selection** from the list
 - g. In the **Credential** field, select the search icon to open the Credentials records list.
 - h. Select **New** to create a new record.
 - i. Select the **API Key Credentials** type.
 - j. In the **API Key** field, enter a name and the API Key provided by your Microsoft Defender for IoT management console.
 - k. Select **Submit** to create the credential record.

To create an API Key in the Microsoft Defender for IoT management console, refer to Microsoft product documentation: <https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis>.

- I. On the Connection form, select **Submit** to finish creating the Connection record.

6. To test the connection, complete the following:
 - a. In the Setup Connections and Credentials section, select the Test/Validate Connection task.

 - b. Select the **Test Connection** UI action from the related links section on the data source record for sensors. After completing the connection test, view the results. You must perform the suggested troubleshooting steps until the test result returns **Success**.

 - c. Check that the connection manager has a valid certificate.

A valid certificate must be installed for a production environment. For a non-production or proof of concept (POC) instance, you can configure the system properties to enable the integration to work when the connection manager doesn't have a valid certificate. The following table lists the system properties that you can configure for a non-production environment.

System properties for a non-production environment

Property	Value
com.glide.communications.httpclient.verify_certificate	false
com.glide.communications.httpclient.verify_trustmanager	false
	If you need to add this system property, see Add a system property .
com.glide.communications.trustmanager_truststore	true

- d. Check the MID security policy.

In the intranet record, verify that the columns in the following table show the specified values.

Intranet record values

Column	Value
Certificate chain check	false
Hostname check	false
Revocation check	false

For more information, see [MID Server certificate check policies](#).

The connection shows that it is set correctly when the progress window shows the Completion code **Success**, and the number of records processed shows as the same number of sensors in the connection manager.

7. To configure the system properties, complete the following:

- In the Configure System Properties section, select **Configure**.
- Configure the following system properties.

Property	Description
sn_msftd4iotsgc.resourcepath.sensor	<p>Set the sensors resource path.</p> <ul style="list-style-type: none"> The sensors resource path is provided by default for the V3 API version. If you want to use a different API version, you can override the path.
sn_msftd4iotsgc.resourcepath.device	<ul style="list-style-type: none"> The devices resource path is provided by default for the V3 API version. If you want to use a different API version, you can override the path.
sn_msftd4iotsgc.resourcepath.connection	<ul style="list-style-type: none"> The connections resource path is provided by default for the V3 API version. If you want to use a different API version, you can override the path.
sn_msftd4iotsgc.pagesize.device	<p>Enter the number of records to display per page for each Devices and Connections API. Default value: 50 records per page</p>
sn_msftd4iotsgc.pagesize.connection	<ul style="list-style-type: none"> If you want to use a different Connection Alias than the Microsoft D4IoT Base API configured while setting up the connections and credentials records, you can enter the sys_id of your custom Connection Alias record in this property field. The default value of this property is empty. If this property field is left blank, the Microsoft D4IoT Base API Connection Alias is used by default.
sn_msftd4iotsgc.get_all_devices	<p>Select whether to fetch all records for devices, or only new records since the start time of the last successful import.</p> <p>Note: When you import devices for the first time, all records are imported regardless of the setting for this property.</p>
sn_msftd4iotsgc.get_all_connections	<p>Select whether to fetch all records for connections, or only new records since the</p>

Property	Description
	<p>start time of the last successful import in the CMDB.</p> <p>Note: When you import connections for the first time, all records are imported regardless of the setting for this property.</p>
sn_msftd4iotsgc.ot.vr.integration.id	<p>If you are using the Operational Technology Vulnerability Response application with the Service Graph for Microsoft Defender for IoT integration, provide the sys ID of the OT VR import record.</p> <p>Note: If the Operational Technology Vulnerability Response plugin is installed and this property field is left blank, the Microsoft D4IoT Devices CVE Integration (Delta Import) executes if Active is set to true on the record.</p>

c. Select **Save**.

8. To import sensors, complete the following:
 - a. In the Configure Sensors (NIDS) section, select the Import Sensors task.
 - b. Select **Configure**.
 - c. Select **Active** to activate the Scheduled Data Import job.
9. To configure the NIDS, complete the following:
 - a. In the Configure Sensors (NIDS) section, select the Import Sensors task.
 - b. Select **Mark as complete** once you complete the NIDS configuration linked in the description.
10. To configure import schedules, complete the following:
 - a. In the Configure Import Schedules section, select **Configure**.
 - b. Select **SG-OT Microsoft D4IoT Sensors Scheduled Import** to review or change the sensors import schedule as needed.
 - By default, the sensors import schedule is configured to run daily at midnight.
 - Import sensors before importing devices or connections.
 - c. Select **Active** to activate the sensors import schedule.
 - d. Select **SG-OT Microsoft D4IoT Devices Scheduled Import** to review or change the devices import schedule as needed.

- By default, the devices import schedule is configured to run daily at midnight.
- Devices are queried by sensor. The Service Graph Connector queries for devices detected by validated sensors. For information about configuring Network Intrusion Detection System (NIDS) appliances, see [Validate the NIDS](#).

- Select **Active** to activate the devices import schedule.
- Select **SG-OT Microsoft D4IoT Connections Scheduled Import** to review or change the connections import schedule as needed.
 - By default, the connections import schedule is configured to run after the devices import runs (**After Parent Runs**).
 - Connections are only imported if both devices (Source & Destination in Microsoft API, or Parent & Child in the CMDB) are already in the CMDB.
 - Import devices before importing connections.

CMDB classes targeted in the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

When you complete the guided setup, you can configure the integration to periodically pull data from a Microsoft Defender for IoT (On-premises Management Console) project. The data is saved in tables that extend from the Configuration item [cmdb_ci] table.

Computer [cmdb_ci_computer]

The following attributes in the Computer [cmdb_ci_computer] table are populated by collected data:

Attribute label	Attribute name
Operation system	os
OS version	os_version
OS domain	os_domain
OS address width	os_address_width

Configuration Item [cmdb_ci]

The following attributes in the Configuration Item [cmdb_ci] table are populated by collected data:

Attribute label	Attribute name
Hardware vendor	manufacturer
Most recent discovery	most_recent_discovery
First discovered	first_discovered
Name	name
Display name	sys_class_name

IP Address [cmdb_ci_ip_address]

The following attributes in the IP Address [cmdb_ci_ip_address] table are populated by collected data:

Attribute label	Attribute name
IP Address	ip_address

Network Adapter [cmdb_ci_network_adapter]

The following attributes in the Network Adapter [cmdb_ci_network_adapter] table are populated by collected data:

Attribute label	Attribute name
MAC address	name, mac, mac_address

OT Control Module [cmdb_ci_ot_control_module]

The following attributes in the OT Control Module [cmdb_ci_ot_control_module] table are populated by collected data:

Attribute label	Attribute name
Firmware version	firmware_version
Model ID	model_id
Rack number	rack_number
Serial number	serial_number
Vendor	vendor
Most recent discovery	most_recent_discovery
First discovered	first_discovered

OT Device Details [cmdb_ot_entity]

The following attributes in the OT Device Details [cmdb_ot_entity] table are populated by collected data:

Attribute label	Attribute name
Purdue level	purdue_level
Asset criticality	asset_criticality

PLC [cmdb_ci_ot_plc]

The following attributes in the PLC [cmdb_ci_ot_plc] table are populated by collected data:

Attribute label	Attribute name
Switch position	switch_position
Switch remote mode	switch_remote_mode

Attribute mapping and classification for the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

The following tables describe the attribute mapping and classification for sensors and devices.

Sensors attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	<ul style="list-style-type: none"> sys_object_source cmdb_ci_nids 	• snk in sys_object_source • correlation_id	Unique ID for the sensor.
name	String	cmdb_ci_nids	name	Name of the sensor.
properties.hostname	String	cmdb_ci_nids	fqdn	Host name of the sensor.
properties.ip	String	cmdb_ci_ip_address	ip_address	IP address of the sensor.
properties.learning	Boolean	cmdb_ci_nids	False or unavailable: Life Cycle Stage (life_cycle_stage) : Operational Life Cycle Stage Status (life_cycle_stage_status) : In Use True: Life Cycle Stage (life_cycle_stage) : Operational Life Cycle Stage Status (life_cycle_stage_status) : Learning	Learning mode status of the IoT sensor.

Sensors attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.mac	String	cmdb_ci_network_interface	mac_address	MAC address of the sensor.
properties.sensorStatus	String	cmdb_ci_nids	connection_state	Status of the IoT sensor.
properties.sensorVersion	String	cmdb_ci_nids	firmware_version	Version of the IoT sensor.
properties.upSinceDate	Date and time as string	cmdb_ci_nids	first_discovered	Startup time.
properties.zone	String	cmdb_ci_nids	zone	Zone of the IoT sensor.

Devices attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/subscription-id>/providers/<providers-id>/location/<location>/deviceGroups/<device-Group>/devices/<name-field>	<ul style="list-style-type: none"> sys_object_source cmdb_ot_entity cmdb_key_value 	<ul style="list-style-type: none"> snk in sys_object_source • discovery_source_id in cmdb_ot_entity 	Unique ID for the device.
resourceGroup	(Empty)	cmdb_key_value	(Empty)	Resource group
tenantId	(Empty)	cmdb_key_value	(Empty)	Tenant ID
properties.authorizedState	String	cmdb_key_value	(Empty)	Authorized state of the device
properties.criticality	String	cmdb_ot_entity	business_criticality	Criticality of the device
properties.deviceName	String	cmdb_ci	name	Name of the device.
properties.deviceSubType	String	cmdb_ci	sys_class_name	Device subtype display name.
properties.firstSeenDate	Date and time as string	<ul style="list-style-type: none"> cmdb_ci cmdb_ci_ot_control_module (if control modules are present) 	first_discovered	First time the device was seen.

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.lastSeen	Date and time as string	<ul style="list-style-type: none"> cmdb_ci cmdb_ci_ot_control_module (if control modules are present) 	most_recent_discovery	Very time the device was seen.
properties.purdueLevel	String	cmdb_ot_entity	purdue_level	Purdue level of the device.
properties.operatingSystem	String	cmdb_ci_computer	os	OS distribution
properties.operatingSystem.version	String	cmdb_ci_computer	os_version	OS version
properties.operatingSystem.platform	String	cmdb_ci_computer	os_domain	OS platform
properties.operatingSystem.architecture	String	cmdb_ci_computer	os_address_width	OS architecture
properties.additionalFields.plcKeyState	Object	cmdb_ci_ot_plc	switch_position	PLC key state
properties.additionalFields.plcRunState	Object	cmdb_ci_ot_plc	switch_remote_mode	PLC run state
properties.hardwareObject	(Empty)	(Empty)	(Empty)	Device hardware data
properties.hardwareModel	String	cmdb_ci	(Empty)	Hardware model
properties.hardwareSerialNumber	String	cmdb_serial_number	serial_number	Hardware serial number
properties.hardwareVendor	String	cmdb_ci	manufacturer	Hardware vendor
properties.nics	Array of Objects	(Empty)	(Empty)	List of the device network interface cards.
properties.nics[{}]	Object	(Empty)	(Empty)	Network interface card properties
properties.nics[{}].ipAddress	String	cmdb_ci_ip_address	ip_address	IPv4 address
properties.nics[{}].macAddress	String	cmdb_ci_network_interface	mac_address	MAC Address
properties.slots	Array of Objects	(Empty)	(Empty)	List of the device slot in the backplane.
properties.slots[{}]	Object	(Empty)	(Empty)	Slot data in PLC backplane.
properties.slots[{}].firmwareVersion	String	cmdb_ci_ot_control_module	firmware_version	Firmware version of the slot.
properties.slots[{}].model	String	cmdb_ci_ot_control_module	model	Model of the slot.

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.slots[{}].rackNumber	Integer	cmdb_ci_ot_controller	rackNumber	Rack number in the backplane
properties.slots[{}].serialNumber	String	cmdb_ci_ot_controller	serialNumber	Serial number of the slot.
properties.slots[{}].slotNumber	Integer	cmdb_ci_ot_controller	slotNumber	Slot number inside the rack.
properties.slots[{}].softwareVendor	String	cmdb_ci_ot_controller	softwareVendor	Hardware vendor of the slot.

Device type classification

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Alarm Siren	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Alarm System	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
ATM	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Backup Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Barcode Scanner	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DB Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
DCS Controller	Industrial	(Empty)	DCS	cmdb_ci_ot_dcs	NULL
Domain Controller	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Door Control Panel	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DVR	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Elevator	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Engineering Station	Industrial	(Empty)	EWS	cmdb_ci_ot_ews	EWS
Fire Alarm	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Fire Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Firewall	(Empty)	(Empty)	IP Firewall	cmdb_ci_ip_firewall	NULL
Game console	(Empty)	(Empty)	Game Console	cmdb_ci_game_console	NULL
Historian	(Empty)	(Empty)	Historian	cmdb_ci_ot_historian	Historian
HMI	Industrial	(Empty)	HMI	cmdb_ci_ot_hmi	HMI

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Humidity Sensor	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
HVAC	(Empty)	(Empty)	HVAC Equipment	cmdb_ci_hvac	NULL
I/O Adapter	(Empty)	(Empty)	Network Adapter	(Empty)	NA
IED	(Empty)	(Empty)	IED	cmdb_ci_ot_ied	ied
Industrial Packaging System	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Industrial Robot	(Empty)	(Empty)	Industrial Robot	cmdb_ci_ot_industrial_robot	Industrial Robot
Industrial Scale	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Intercom	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
IP Camera	(Empty)	(Empty)	IP Camera	cmdb_ci_ip_camera	NULL
IP Telephone	(Empty)	(Empty)	IP phone	cmdb_ci_ip_phone	NULL
Marquee	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Meter	(Empty)	(Empty)	Industrial Sensor	cmdb_ci_ot_industrial_sensor	Industrial Sensor
Motion Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Multicast/Broadcast	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
NTP Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
People Counter System	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Physical Location	(Empty)	(Empty)	(Empty)	(Empty)	NULL
PLC	Industrial	(Empty)	PLC	cmdb_ci_ot_plc	PLC
Pneumatic Device	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Printer	(Empty)	(Empty)	Printer	cmdb_ci_printer	NULL
Protocol Converter	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Punch Clock	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Robot Controller	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
Router	(Empty)	(Empty)	IP Router	cmdb_ci_ip_router	NULL
RTU	(Empty)	(Empty)	RTU	cmdb_ci_ot_rtu	NULL
Server	Server	(Empty)	Server	cmdb_ci_server	NULL
Servo Drive	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Slot	(Empty)	(Empty)	OT Control Module	cmdb_ci_ot_control_module	OT Control Module
Smart Light	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart Phone	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Smart Switch	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart TV	(Empty)	(Empty)	Smart Television	cmdb_ci_stv	NULL
Storage	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Switch	Network Device	(Empty)	IP Switch	cmdb_ci_ip_switch	NULL
Tablet	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Terminal Station	(Empty)	(Empty)	Computer	cmdb_ci_computer	NULL
Thermostat	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Turnstile	(Empty)	(Empty)	IoT device	cmdb_ci_iot	
Uninterruptable Power Supply	(Empty)	(Empty)	UPS	cmdb_ci_ups	NULL
Variable Frequency Drive	(Empty)	(Empty)	Industrial Drive	cmdb_ci_ot_industrial_drive	Industrial Drive
VPN Gateway	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wifi Pineapple	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wireless Access Point	(Empty)	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL
WLAN access point	Network Device	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Workstation	Workstation	(Empty)	Computer	cmdb_ci_computer	NULL
Unknown	All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Unclassified	Unclassified or All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any other type	(Empty)	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • windows server • windows server, version 2004[8] • windows server, version 1909[9] • windows server, version 1903[9] • windows server 2019 • windows server 2016 • windows server 2012 r2 • windows server 2012 • windows server 2008 r2 • windows server 2008 • windows server 2003 r2 • windows server 2003 	Windows Server	cmdb_ci_linux_server	Same as when the operating system isn't present.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
		<ul style="list-style-type: none"> • windows 2000 server • windows nt 4.0 server • windows nt 3.51 server • windows nt 3.5 server • windows nt 3.1 server 			
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • linux • arch • centos • debian • fedora • suse • red hat • rhel • ubuntu • oracle 	Linux Server	cmdb_ci_linux_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	aix	AIX Server	cmdb_ci_aix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	esx	ESX Server	cmdb_ci_esx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> • hp/ux • hpx 	HP-UX Server	cmdb_ci_hpx_server	Same as when the operating system isn't present.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> hyper-v hyperv hyper 	HypverV Server	cmdb_ci_hyper_v_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> solaris sunos sun os 	Solaris Server	cmdb_ci_solaris_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> macos x server macos server os x osx 	OSX Server	cmdb_ci_osx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> unix gnu 	Unix Server	cmdb_ci_unix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	<ul style="list-style-type: none"> win windows Microsoft windows 1.0, 1.02, 1.03, 1.04, 2.03, 2.10, 2.11, 3.0, 3.1, 3.2, 7, 8, 8.1, 10, 98, 95 windows 2000 windows for workgroups 3.11 	Base Computer class	cmdb_ci_computer	Same as when the operating system isn't present.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/firmware	NOW class	NOW table	NOW OT type
		<ul style="list-style-type: none"> • windows me • windows nt 3.1, 3.5, 3.51, 4.0 • windows vista • windows xp • windows xp professional x64 edition 			
Any above type value except with designation Network and IoT	(Empty)	server	Base Server Class	cmdb_ci_server	Same as when the operating system isn't present.

Using the Operational Technology Manager

After you complete all required set up tasks, including installing the Operational Technology (OT) extension classes and assigning user roles, perform the following tasks to create the foundational data and relationships for the ServiceNow® Operational Technology solution.

Task	Purpose
1. Populate a Microsoft Excel spreadsheet with your existing Operational Technology data.	Positions your existing data in the correct columns on a Microsoft Excel spreadsheet to ensure the success of your data upload.
2. Import your Excel spreadsheet.	Uploads your existing Operational Technology data to the Configuration Management Database (CMDB).
3. Run the Discovery for Operational Technology function.	Discovers Operational Technology (OT) devices in designated Purdue levels in your Industrial Control System (ICS) networks
4. Use the selections on the Operational Technology (OT) menu.	Enables editing or viewing detailed information for the OT devices in your enterprise.

Service Graph Connector for Operational Technology (Excel)

The Service Graph connector (Excel) function enables you to import your existing Operational Technology data from a populated Microsoft Excel flat-file spreadsheet. You use

it in the Integration Hub Extract Transform Load (ETL) to upload this data to the Configuration Management Database (CMDB).

Before you can run the import process, you must populate the Microsoft Excel spreadsheet with your existing Operational Technology data. When you import your Microsoft Excel spreadsheet using the Integration Hub ETL, it creates the correct configuration item (CI) records in the Configuration Management Database (CMDB). To learn more, see [Operation Technology \(OT\) extension classes](#).

Related topics

[IntegrationHub](#)

[IntegrationHub ETL](#)

Configuring Service Graph Connector for Microsoft Excel

Configure the Service Graph Connector for Microsoft Excel to import your existing Operational Technology data from a populated Microsoft Excel flat-file spreadsheet.

Use the Service Graph Connector for Microsoft Excel guided setup and complete tasks in sequence to configure the Service Graph Connector for Microsoft Excel.

Navigate to **All > Industrial Workspace Admin > Guided Setup**, open the following guided setups, and complete the tasks.

For more information on using guided setup, see [Guided Setup](#).

Task	Purpose
Users	Assigns roles to control the actions that are available for each user.
Staging table configuration	Configure to determine which factors constitute in identifying a unique name for a CI. For more information on system properties, see System properties that impact SG-OT Device Excel Import processing .
Prepare Data	Create and prepare the spreadsheet by positioning your existing data in the correct columns. For more information to prepare the data, see Prepare your Pre-import OT worksheet entry review tool for Service Graph Connector import .
Create new OT devices	Create a new OT Device manually by clicking on the New button from the list view of the Staging table. For more information about creating new OT devices, see
Validate records	Run validations against the imported data to update the Validation stage of the records and provide validation comments.

Task	Purpose
	<p>Note: You don't need to select any records on the list to run validations. Validations are run on all the records present in the staging table.</p> <p>For more information about validating records, see Managing Validations.</p>
Schedule Import	Import data from the staging table to the import set table and review it in the OT list views and Workspace.

Assign Pre-import OT Worksheet Entry Review roles

Assign roles to the users# or user groups so that you can manage the Excel Service Graph Connector staging table and ETL.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the Operational Technology Manager application.

Role	Description
Administrator [cmdb_inst_admin]	<ul style="list-style-type: none"> Can view or edit the ETL. Can view the records in the staging table.
Administrator [cmdb_OT_admin]	Can view or edit the records in the staging table.

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See User Administration
Assign a role to a group	See Group Administration

Preview existing OT records in the CMDB

Preview existing Operational Technology (OT) device records in the Configuration Management Database (CMDB) before you import any new records from the staging table. By previewing existing records, you can avoid reconciling or merging unrelated records.

Before you begin

Role required: cmdb_ot_admin or admin

About this task

If a matching configuration item (CI) is in the CMDB when you import OT devices from the staging table, existing records may reconcile or merge with new records. Matching CIs

include the hostname, MAC address, or serial number. To avoid accidentally reconciling or merging records, you can preview the existing records that share the matching CIs with the records in the staging table.

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Staging Table**.

The validation comments explain the matching CI that was found and contain a link to the matching CI. When a matching CI is found in the CMDB, the Validation state is set to **Partially Valid**. The following table lists the matching CI validation comments.

Matching CI validation comments

Matching CI	Validation comment
Hostname	Same transformed name found for another CI:<Link to CI>
MAC address	Same MAC address [MAC address] found for another CI:<Link to CI>
Serial number	Same serial number [serial number] found for another CI:<Link to CI>

2. Optional: View the matching CI by selecting it from the Matching CI in the CMDB column.

Easy import

Easy import is a simplified import process that enables you to import only the columns that you want.

Only users with the admin role can use easy import. You can import data to tables within the current scope and tables that grant write access to other applications.

Download the Excel template

Download the Microsoft Excel template to create and populate a Microsoft Excel spreadsheet with your existing Operational Technology data.

Before you begin

Role required: admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Staging table**.
2. Right-click the column heading and select **Import** from the list menu.
3. Select if you want to **Insert** or **Update** records.

Import template

Template	Description
Insert	Use this template to add new records to a table.
Update	Use this template to change values within existing records in a table. This template contains one row for each record in the list. The current list filter determines what records the template contains.

(i) Insert new records or update existing records using an Excel template file. Click Upload to preview the data to be imported. [More Info](#)

[Import external data into SG OT Excel Staging](#)

Do you want to insert or update data ? Insert Update

Do you want to create an Excel template to enter data ?

Step 1: Create an Excel template file to enter data

Include all fields in the template?

[Create Excel template](#)

Step 2: Upload the template file

Excel template file No file chosen

[Upload](#)

- Clear the **Include all fields in the template** check box to include only the columns that appear in the list in the template.

Certain fields in the table are updated by system processes and you cannot import values into them. An example is the **Created by** field, which is populated during import with the logged-in user who performs the import.

Leave this check box selected to include all columns from the table in the template, even those columns that are hidden in the list.

- Select **Create Excel template**.
- In the Export Complete page, select **Download** to download the Microsoft Excel spreadsheet.

What to do next

Open the spreadsheet using your preferred application.

Note:

The template contains a **Directions** tab describing how to use the template.

Prepare your Pre-import OT worksheet entry review tool for Service Graph Connector import

Prepare your spreadsheet by positioning your existing data in the correct columns is crucial to the success of your upload.

Before you begin

Role required: admin

About this task

Procedure

- Fill the following columns in the Microsoft Excel spreadsheet:

Note: Column names cannot be changed. Extra columns can be added to the staging table. For more information about adding a new custom field mapping in the staging table, see [Add a custom field mapping in the staging table for Service Graph](#).

Refer to the following tables for guidance while filling in the spreadsheet. The spreadsheet contains many columns. The examples and field descriptions are split into multiple sections.

- Filling in columns A through K
- Filling in columns L through Y
- Filling in columns Z through AI
- Filling in columns AJ through AT
- Filling in columns AU through BD
- Filling in columns BE through BR
- Filling in columns BS to BW

Columns A through K

Column	Required column name	Type	Description and example
A	Device criticality	string	<p>Measure of how critical, or important, the OT device is, based on its role. Examples:</p> <ul style="list-style-type: none"> ◦ High or Most critical ◦ Medium or somewhat critical ◦ Low or Less critical ◦ None or not critical
B	Assigned to	string	Email address of the user that this OT device is assigned to. For example: bob@example.com
C	Backplane id	string	Unique ID that is used for the identification of the backplane and mapping to control modules. For example: BPSN123
D	Backplane name	string	Name of the backplane, if any, for the OT device. Examples: Backplane #51, PLC1 Backplane
E	Control module parent id	string	Unique ID that is used for the identification of the control modules to the parent control system backplane. For example: 482bb239-05e8-4bad-ba59-925eb87ff06e
F	Correlation id	string	Unique ID that is used for identification of the OT device. Enter the correlation_id a string. Examples: 482bb239-05e8-4bad-ba59-925eb87ff06e or 5123456. This column entry is required.

Column	Required column name	Type	Description and example
			<ul style="list-style-type: none"> Each imported OT device must have a correlation_id that is unique. The OT device data that you import normally originates in an external source system, which usually assigns a unique identifier to each record.
G	Custom field 1	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes. Examples: Refurbished, Used
H	Custom field 2	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes. Examples: Painting, Stamping
I	Custom field 3	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes.
J	Custom field 4	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes.
K	Custom field 5	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes.

Columns L through Y

Column	Required column name	Type	Description and example
L	Display name	string	Used to populate the display name of OT devices.
M	Equipment model entity path	string	Path of the equipment model entity that the OT device is mapped to.
N	Firmware version	string	Firmware version of the OT device, if any. For example: 12.0
O	First discovered	datetime	ISO-formatted timestamp of the first time that the OT device was

Column	Required column name	Type	Description and example
			first discovered on your network. For example: YYYY-MM-DD HH:MM:SS.
P	Hardware version	string	Hardware version of the OT device, if any. For example: 13.2
Q	Has module	Boolean	For control systems with modules, indicates that this system has modules. Examples: True, False
R	IO field device type	string	If this device is a field device, indicates if it is used for input, output, or both. Examples: <ul style="list-style-type: none">◦ input◦ output◦ input_output The device acts as both input and output.
S	IP Address 1	string	First IP address, if any, that is associated with the OT device. If there are multiple IP addresses, use the next IP address column (IP Address 2). Examples: 10.0.0.22, 10.0.0.12
T	IP Address 2	string	Second IP address, if any, that is associated with the OT device. Examples: 192.168.100.1, 192.168.100.5
U	IP Address 3	string	Third IP address, if any, that is associated with the OT device.
V	IP Address 4	string	Fourth IP address, if any, that is

Column	Required column name	Type	Description and example
			associated with the OT device.
W	IP Address 5	string	Fifth IP address, if any, that is associated with the OT device.
X	IP Address 6	string	Sixth IP address, if any, that is associated with the OT device.
Y	IP Address 7	string	Seventh IP address, if any, that is associated with the OT device.

Columns Z through AI

Column	Required column name	Type	Description and example
Z	IP Address 8	string	Eighth IP address, if any, that is associated with the OT device.
AA	IP Address 9	string	Ninth IP address, if any, that is associated with the OT device.
AB	MAC Address 1	string	First MAC address, if any, that is associated with the OT device. If there are multiple MAC addresses, use the next Mac address column (MAC Address 2). Examples: 94:94:1d:01:6d:5f, cc:7c:4a:fb:20:71

Column	Required column name	Type	Description and example
			<p>Note: For an OT device, you must create an entry in at least one of these three spreadsheet columns, all values in these columns must be unique for the spreadsheet:</p> <ul style="list-style-type: none"> ◦ MAC Address 1 ◦ Name ◦ Serial number
AC	MAC Address 2	string	Second MAC address, if any, that is associated with the OT device. For example: e5:4d:c8:36:b1:2d
AD	MAC Address 3	string	Third MAC address, if any, that is associated with the OT device.
AE	MAC Address 4	string	Fourth MAC address, if any, that is associated with the OT device.
AF	MAC Address 5	string	Fifth MAC address, if any, that is associated with the OT device.
AG	MAC Address 6	string	Sixth MAC address, if any, that is associated with the OT device.
AH	MAC Address 7	string	Seventh MAC address, if any, that is associated with the OT device.
AI	MAC Address 8	string	Eighth MAC address, if any, that is associated with the OT device.

Columns AJ through AT

Column	Required column name	Type	Description and example
AJ	MAC Address 9	string	Ninth MAC address, if any, that is associated with the OT device.
AK	Manufacturer	string	Name of the manufacturer of the OT device. Examples: Rockwell Automation, Dell
AL	Memory card serial 1	string	Assigned serial number of the first memory card, if any, that is installed in the OT device. If there are multiple memory cards, use the next memory card serial column (Memory card serial 2). Examples: MMC DA362131, MemSN123
AM	Memory card serial 2	string	Assigned serial number of the second memory card, if any, that is installed in the OT device. For example: MemSN123
AN	Memory card serial 3	string	Assigned serial number of the third memory card, if any, that is installed in the OT device.
AO	Memory size 1	string	Size of the first memory card, if any, that is installed in the OT device. Examples: 256 GB or 1 GB
AP	Memory size 2	string	Size of the second memory card, if any, that is installed in the OT device. Examples: 256 GB or 1 GB
AQ	Memory size 3	string	Size of the third memory card, if any, that is installed in the OT device. Examples: 256 GB or 1 GB
AR	Memory type 1	string	Type of memory card that is installed in the OT device. If there are multiple memory cards, use multiple columns. For example: RAM
AS	Memory type 2	string	Type of memory card that is installed in the OT device. Examples: RAM
AT	Memory type 3	string	Type of memory card that is installed in the OT device.

Columns AU through BD

Column	Required column name	Type	Description and example
AU	Model number	string	Manufacturer's model number for the OT device. Examples: ThinkServer TD230, XPS 15z
AV	Module type	string	Description of the function of the control module, if this device is one. Examples: Input, Output
AW	Name	string	Host name of the OT device, usually as part of the FQDN. Examples: PLC1, Door Assembly HMI, and Robot Control Module.

Column	Required column name	Type	Description and example
			<p>Note: For an OT device, you must create an entry in at least one of these three spreadsheet columns. All values in these columns must be unique for the spreadsheet:</p> <ul style="list-style-type: none"> ◦ MAC Address 1 ◦ Name ◦ Serial number
AX	Operating system	string	<p>Operating system, if any, that is installed on the OT device. Examples: Linux Fedora, Windows 10, Windows 2000, Mac OS 8.</p> <p>Note: For an OT device, you should create entries in the following spreadsheet columns, even though they are not required:</p> <ul style="list-style-type: none"> ◦ Type ◦ If available, Operating System ◦ If available, Firmware version
AY	OS version	string	<p>Reported version of the operating system, if any, that is installed on the OT device. Examples: 10.0, 13.5.2</p> <p>Note: For an OT device, you should create entries in the following spreadsheet columns, even though they are not required:</p> <ul style="list-style-type: none"> ◦ type ◦ If available, os_version ◦ If available, firmware version
AZ	OT Staging Task	string	Tasks created to remediate invalid records on the staging table.
BA	Purdue level	string	Assigned Purdue level for the OT device. Assigning a Purdue level ensures that the Discovery for the Operational Technology function properly locates each item at the correct ICS level and produces accurate Discovery results. Examples: 1, 2, 3
BB	Rack number	string	Rack where the control module is mounted. Examples: 1, 2, 3
BC	Serial number	string	Assigned serial number, if any, for the OT device. Examples: SN545, SN998

Column	Required column name	Type	Description and example
			<p>Note: For an OT device, you must create an entry in at least one of these three spreadsheet columns. All values in these columns must be unique for the spreadsheet:</p> <ul style="list-style-type: none"> ◦ MAC Address 1 ◦ Name ◦ Serial number
BD	Serial number type	string	Normally set to the value of "system," but it could be a different type of serial number. For example: uuid

Columns BE through BR

Column	Required column name	Type	Description and example
BE	Short description	string	Short description of the OT device. Examples: HMI for the Door Painting Cell, Controls the door assembly robot.
BF	Site	string	<p>The equipment models start at the site level and contain a detailed hierarchical structure that describes each industrial site.</p> <p>For more information, see ISA-95 equipment model.</p>
BG	Slot number	string	For a control module, indicates the slots that this device occupies in the chassis of the control system. Examples: 1, 2
BH	Software install date 1	datetime	<p>Date that the application software was installed on the OT device. If there are multiple dates, use multiple columns.</p> <p>Use only UTC format for the date.</p> <p>For example: YYYY-MM-DD HH:MM:SS</p>
BI	Software install date 2	datetime	<p>Date that the application software was installed on the OT device. If there are multiple dates, use multiple columns.</p> <p>Use only UTC format for the date. For example: YYYY-MM-DD HH:MM:SS</p>
BJ	Software install date 3	datetime	<p>Date that the application software was installed on the OT device. If there are multiple dates, use multiple columns.</p> <p>Use only UTC format for the date. Example: YYYY-MM-DD HH:MM:SS.</p>

Column	Required column name	Type	Description and example
BK	Software installed 1	string	Name of the application software, if any, that is installed on the OT device. If there are multiple names, use multiple columns. For example: Rockwell HMI Vision
BL	Software installed 2	string	Name of the application software, if any, that is installed on the OT device.
BM	Software installed 3	string	Name of the application software, if any, that is installed on the OT device.
BN	Software version 1	string	Reported version of the application software, if any, that is installed on the OT device. If there are multiple versions, use multiple columns. For example: v1.2 or v2011 SP3 HF2 or 4.54.32145
BO	Software version 2	string	Reported version of the application software, if any, that is installed on the OT device. For example: v1.2 or v2011 SP3 HF2 or 4.54.32145
BP	Software version 3	string	Reported version of the application software, if any, that is installed on the OT device. For example: v1.2 or v2011 SP3 HF2 or 4.54.32145
BQ	Status	string	<p>Status of the OT device:</p> <p>--None--</p> <p>No assigned status.</p> <p>Absent</p> <p>OT device is absent in your facilities.</p> <p>In Maintenance</p> <p>OT device is in maintenance and currently is off line.</p> <p>In stock</p> <p>OT device is in stock in your facilities.</p> <p>Installed</p> <p>OT device is installed in your facilities.</p> <p>Pending Install</p> <p>OT device is pending installation in your facilities.</p> <p>Pending repair</p> <p>OT device is pending repair but is not online yet.</p> <p>Retired</p> <p>OT device is retired.</p> <p>Stolen</p>

Column	Required column name	Type	Description and example
			OT device has been stolen.
BR	Support group	string	Name of the primary support group for this OT device. Examples: Door Support, Corporate IT Support.

Columns BS to BW

Column	Required column name	Type	Description and example
BS	Transformed name	string	<p>Users must not fill this column.</p> <p>By default, the transformed name value is populated using transformed column system properties.</p> <p>A user cannot edit the Transformed name.</p> <p>For system properties, see System properties that impact SG-OT Device Excel Import processing.</p>
BT	Type	string	Type of OT device/configuration item (CI). Examples: PLC, DCS

Column	Required column name	Type	Description and example
			<p>i Note:</p> <ul style="list-style-type: none"> ◦ For a listing and explanation of valid CI types, see Operation Technology (OT) extension classes. ◦ For an OT device, you should create entries in the following spreadsheet columns, even though they are not required: <ul style="list-style-type: none"> ▪ type ▪ os_version
BU	Validation comments	string	<p>Users must not fill this column.</p> <p>By default, Validation comments are populated after the validations are run on the staging table records that are imported from excel.</p> <p>Validation comments are not updated when records are imported.</p> <p>User cannot edit the Validation comments.</p>
BV	Validation state	string	Users must not fill this column.

Column	Required column name	Type	Description and example
			<p>By default, the validation state is populated when the data is imported in the staging table.</p> <p>Status of the OT device:</p> <ul style="list-style-type: none"> Pending validation Default state when records are imported into the staging table. Invalid Cannot uniquely create a CI record in the CMDB. Partially valid One of the Transformed Name, MAC Address 1, and Serial number has no value. All the other fields (correlation id, control module parent id) have values. Valid

Column	Required column name	Type	Description and example
			<p>All identifiers are present and are ready for import.</p> <p>Imported</p> <p>Completed the import of the data from the staging table to the Import set table.</p> <p>User cannot edit the Validation state.</p>
BW	Vendor	string	Name of the vendor of the OT device.

- After populating the Microsoft Excel spreadsheet, save it in a known location for easy access to upload.

System properties that impact SG-OT Device Excel Import processing

The SG-OT Device Excel Import process depends on the following system properties for successful completion.

sn_otsm_sgc.excel.fields.for.transformed.name

- This property enables the user to provide the fields to construct the transformed name.
- The field value or column names must be separated by comma.

This transformed name is used as the name of the configuration item (CI) instead of the name field directly from the staging table. By default, the name field value is itself used as the transformed name value.

- This property belongs to the **sn_otsm_sgc** scope and is automatically appended to this property name.
- Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.

sn_otsm_sgc.excel.transformed.name.delimiter

- This property specifies the delimiter to be used when computing the transformed name with more than one field or column value specified in the system property **fields.for.transformed.name**.
- If only one column name is specified in the **fields.for.transformed.name** property, the delimiter is not used.
- This property belongs to the **sn_otsm_sgc** scope and is automatically appended to this property name.
- Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.

sn_otsm_sgc.excel.fields.for.validation.state.change

- This property enables you to provide a comma-separated list of attributes so that their validation state is changed to **Pending validation**. The default value is **Empty**.
- i Note:** Changes to the identifier fields, such as Mac Address, Serial Number, Transformed Name, and slot number (for OT control modules), the validation state is changed to **Pending validation**.
- This property belongs to the sn_otsm_sgc scope and is automatically appended to this property name.
 - Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.

sn_otsm_sgc.enable.cmdb.validations

- This property enables CMDB validations for the staging devices. If set to **True**, staging devices are validated against existing CMDB CIs for reconciliation.
- This property belongs to the sn_otsm_sgc scope and is automatically appended to this property name.
- Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.

Import the Excel template

After updating the import template with the new data, import the template to your instance to validate and find missing, duplicate, and invalid data.

Before you begin

Role required: admin

Procedure

1. Navigate to All > Industrial Workspace Admin > OT Manager > Import OT Devices - Staging table.
2. Right-click the column heading and select **Import** from the menu.

The screenshot shows a web-based configuration interface for importing data into a staging table. At the top, there's a note: "Insert new records or update existing records using an Excel template file. Click Upload to preview the data to be imported. [More Info](#)". Below this is a back arrow and the title "Import external data into SG OT Excel Staging".

Two radio buttons are present: "Insert" (selected) and "Update". A checked checkbox indicates the intent to "Create an Excel template to enter data".

Step 1: Create an Excel template file to enter data

A checked checkbox indicates "Include all fields in the template?". A green-bordered button labeled "Create Excel template" is visible.

Step 2: Upload the template file

An "Excel template file" input field contains "Choose file" and "No file chosen". A green-bordered "Upload" button is located below it.

3. Select **Insert** or **Update** as the import type.
4. Select **Choose file** to select the Microsoft Excel spreadsheet.
5. Select **Upload** to upload the Microsoft Excel spreadsheet.
6. In the Upload Progress page, select **Preview Imported Data** to verify the imported data.
7. If the template passes validation and the imported preview matches your expectations, select **Complete Import** to import data into the staging table.

Create an OT device

Create an OT device manually in the Import OT Devices staging table.

Before you begin

Role required: ot_staging_user, cmdb_ot_admin, or admin

Procedure

1. Navigate to All > Industrial Workspace Admin > OT Manager Admin > Import OT Devices - Staging Table.
2. Select the **New** button.
3. From the **What is the type of the device?** list, select the OT device type. The device type that you select is automatically added to the form.
4. On the **SG OT Excel Staging - New Record** form, fill in the fields as needed.

SG OT Excel Staging - New Record form fields

Field	Description
Display name	The name of the OT device displayed in the record. i Note: You can add any string value to this field. Multiple devices can have the same OT display name. This is meant for easier understanding of the OT device and is different from the unique CI name generated when you import OT devices from the staging table.
Name	Unique CI generated name.
Purdue level	Assigned Purdue level. The level ranges are 0–5. i Note: To learn more about the Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems .
Device criticality	Measure of the relative risk to the site process if the device fails: <ul style="list-style-type: none"> ◦ 1 - Most critical ◦ 4 - Not critical
Correlation id	Site that the device belongs to.
Site	The top-level parent entity, or industrial site, where the device is located or assigned to.
Equipment model entity path	Equipment model entity path that the device is on.

5. Optional: Add any additional info in the following related lists as needed.

- Additional Info
- Network Adapters
- IP Address
- Serial Number
- OS Info
- Control System Info
- Control Module Info

- Software Info
- Memory Module Info

6. Select **Create OT Device**.

Result

The OT device is created and added to the staging table.

Managing Validations

Validation enables you to review and manage the imported data in the staging table.

Validations to be executed:

- Missing correlation id (Correlation id)
- Missing parent correlation id in case the type is Control module (Control module parent id)
- Missing serial number (Serial number)
- Missing transformed name (Transformed name)
- Missing MAC Address (validation is executed on column MAC Address 1)
- Missing type (Type)
- Missing rack number (Rack number)
- Missing slot number (Slot number)
- Equipment model entity path does not exist (Equipment model entity path)
- Site name provided is invalid (Site name)
- Validate duplicates on transformed name (Transformed name)

i Note: This validation is skipped for control modules.

- Validate duplicates on MAC Address (check on all MAC Address 1 columns)
- Validate duplicates on Serial number column (Serial number)
- Validate duplicates on Correlation id column (Correlation id)
- Validate duplicates on rack and slot numbers

i Note: This validation is only for control modules.

- Validate Has Module and Control module Parent ID

i Note: This validation is only for PLCs and control modules.

- Validate Invalid types - Compare against the default Excel type to OT device type mapping through the `sn_otsm_sgc.SGOTAssetImportExtensionPoint` extension point implementation.

If you have additional mappings, create an extension point implementation for the base system `sn_otsm_sgc.SGOTAssetImportExtensionPoint` extension point.

For more information about adding a custom implementation for device classification, see [Add a custom implementation for device classification](#).

Run Validations

Run validations on records to find missing, duplicate, and invalid data.

Before you begin

Role required: ot_staging_user, cmdb_ot_admin, or admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Staging table.**

2. Select Run Validations to trigger validations in the staging table.

Validations are run in the background for all records.

The time that it takes to validate the data depends on the number of records present in the staging table.

3. After the validation is complete, check the status of the record in the Validation state column in the staging table.

4. If the status of the record is partially valid or invalid, do the following:

- a. Check for the missing data in the record.

- b. Make corrections in the record.

The record can be edited in the staging table list view and in the record for view.

- c. Update the record.

- d. Run the validations.

5. If the missing data is not available, do the following to override the state for the specific record to manually set that record as valid:

- a. Select the record to open the form.

- b. Select **Set to Valid**.

 **Note:**

If any record is manually set as valid, it may cause reconciliation issues and a CI might not get created.

Use OT staging tasks to remediate invalid records

Remediate invalid records in the SG OT Excel Stagings table by using Operational Technology (OT) staging tasks. Using OT staging tasks can help you track the invalid records that you need to fix.

Before you begin

Role required: cmdb_ot_admin, cmdb_ot_editor, and ot_staging_user

About this task

You can use OT staging tasks to remediate your invalid records in the SG OT Excel Stagings (sg_ot_excel_staging) table.

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager Admin > Import OT Devices - Staging Table.**

2. In the table header, select the **Create tasks** button.

The following confirmation message appears.

(i) Staging task creation process for all the invalid records have started in the background. It may take few minutes to complete.

3. Wait for the staging task creation process to complete.

After the staging task creation is complete, the OT Staging Task column in the table is filled in with the OT staging tasks that are related to the invalid staging records.

4. Review and edit the staging task record.

- In the OT Staging Task column, select a record.
- On the staging task record form, fill in the fields if applicable.

OT staging task record form

Field	Description
State	State of the staging task. The state moves and tracks the staging tasks through several stages of remediation.
Site	Site that the staging task is associated with. The default staging task record has an empty Site field. All invalid staging records with empty or invalid Site fields are associated with the default staging task. i Note: If you change the Site field on a staging record, the related staging task record is removed.
Description	Detailed explanation of the staging task.
Opened by	User that created the staging task record.
Assigned to	User who works on the staging task.
Assignment group	Assigned group that works on the staging task.

c. Select Update.

5. Optional: View the OT staging task records that were created in the SG OT Excel Stagings Tasks (sg_ot_excel_staging_task) table by navigating to **All > Industrial Workspace Admin > OT Manager Admin > Import OT Devices - Staging Task Table**.

Result

The staging task record is now created and assigned to the user who is responsible for remediation.

Schedule the time interval to import data

Schedule the time interval to import the data from the staging table to the CMDB.

Before you begin

Role required: admin or cmdb_inst_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Staging table**.
2. In the SG OT Excel Staging page, select **Scheduled import**.
3. Select the **Active** check box to schedule the time interval to import the data.
4. Select **Execute Now** to import the record from the staging table to the CMDB.

The Validation state shows the **Imported** status for successfully imported data.

In the staging table, the table cleaner deletes all records that are successfully imported. For more information about table cleaner, see [Table cleaner](#).

Import your Microsoft Excel spreadsheet using the staging table

Import your Microsoft Excel spreadsheet into the staging table using easy import to create the required data in the staging table from the spreadsheet.

Before you begin

This process requires the IntegrationHub ETL (com. sn_int_studio) plugin.

Before you perform this process, you must properly prepare a Microsoft Excel spreadsheet for import. To learn more, see [Prepare your Pre-import OT worksheet entry review tool for Service Graph Connector import](#).

When the data is ready to be imported, you can schedule the import into the Configuration Management Database (CMDB). This process creates unique records in the Configuration Management Database (CMDB) for the OT devices that are included in your spreadsheet.

Roles required: cmdb_inst_admin, import_admin, import_scheduler, admin

About this task

When you run the Integration Hub Extract Transform Load (ETL), you can also refer to the embedded content in the Industrial Guided Setup for additional assistance.

Execute the validations in the staging table to check for duplicates and inconsistencies in the data.

To access the Industrial Guided Setup, navigate to **Industrial Workspace Admin > Guided Setup**.

Procedure

1. Navigate to **All > Configuration > IntegrationHub ETL**.
2. Select the **CMDB Application: SG-OT Excel Import** ETL.
3. On the ETL Transform Map Assistant form, select **Import Source Data and Basic Details**.
4. On the Provide Basic Information for the ETL Transform Map form, in the **Sample Import Set** field, select **Auto-pull a new import set**.
5. Return to the Integration Hub ETL form.

Note: The remaining steps for creating an ETL transform map are automatically completed. However, you can select a specific step to review it before performing the actual import. For example, select **Prepare and Preview Data** to view the nested data structure and raw source data.

Note: For more details, see [Create an ETL Transform Map](#).

6. To perform the actual Excel spreadsheet import, select **Test and Rollback Integration Results**.

7. Select **Run Integration**.

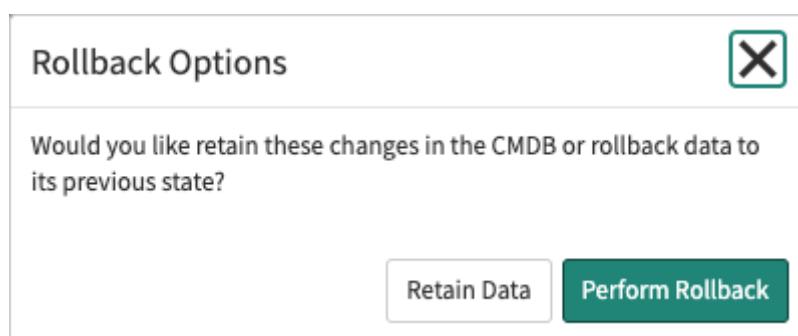
Note: This import tests 100 records. To run a full import of more than 100 records, you must schedule the import. You can schedule the import to run on a regular set schedule by selecting **Set Import Schedule**.

After the data import is complete, the Test and Rollback Integration Results form appears with import statistics, including:

- Classes Mapped
- Relationships between classes
- New Records created from this integration run.
- Records updated from this integration run.
- Partial records created from this integration run.
- Incomplete records created from this integration run.

8. Exit the Test and Rollback Integration Results form.

The Rollback Options dialog box is displayed.



9. Select **Retain Data** to retain the imported data, or select **Perform Rollback** to roll back the imported data and reattempt the Microsoft Excel import.

10. To formally import your spreadsheet data to the Now Platform:

a. Select **Set Import Schedule**.

b. Select **Set Schedule**.

c. In the Scheduled Data Imports list, select **SG-OT Devices Schedule Import using Spreadsheet**.

d. On the Schedule Data Import form, select **Execute Now**.

What to do next

After all steps are completed, from the SG-OT Device Import ETL Guided setup homepage, select **Activate** to activate the ETL.

Add a custom field mapping in the staging table for Service Graph

Add a custom field to the staging table and map the custom field from the staging table to the CI field through Excel SGC.

Before you begin

To configure the form layout, see [Configure the form layout](#).

To create a custom field on the staging table, see [Add and customize a field in a table](#).

Roles required:

- admin - Can make changes in the script include, and add class or field mappings and make changes in the ETL.
- cmdb_inst_admin - Can only add new class or field mappings and make changes in the ETL.

Procedure

1. After a custom column is created in the staging table, navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Staging table**.
2. Download the Excel template.
For more information, see [Download Excel template](#).

If records are present in the staging table, you can edit the value for the column in the existing records.
3. Prepare the Excel template.
For more information, see [Preparing your Pre-import OT worksheet entry review tool for Service Graph Connector import](#).
4. Import the Excel template.
For more information, see [Import Excel template](#).
5. Navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Script Includes** and select the SGOTAssetImportExcelConstants script include.
6. In the script, update the new column name from the staging table, and the new ETL column name inside the SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap object in the format "<ETL Column Name>": "<Column Name from staging table>".

In this example, the "u_my_custom_field" before the colon (:) indicates the ETL column name (shown as a column in the ETL preview step), and the "u_my_custom_field" after the colon indicates the column name in the staging table.

Make sure that there is a comma (,) added at the end of the line above the new line. In this example, a comma is added after the "custom_fields": "custom_fields" line.

```

SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap = {
    // unique id used to uniquely identify the asset
    "id": "correlation_id",
    // Name of the asset
    "name": "transformed_name",
    // OperatingSystem of the asset
    //"operating_system": "os_version",
    // type of the asset.
    "type": "type",
    // if the asset has control module
    "has_module": "has_module",
    // id of the asset to which a control module belongs to (this is used in control module type asset).
    "control_module_parent_correlation_id": "control_module_parent_correlation_id",
    "ot_display_name": "display_name",
    "serial_number": "serial_number",
    "firmware_version": "firmware_version",
    "os_version": "os_version",
    "operating_system": "os",
    "assigned_to": "assigned_to",
    "manufacturer": "manufacturer",
    "model_number": "model_number",
    "serial_number_type": "serial_number_type",
    "purdue_level": "purdue_level",
    "asset_criticality": "asset_criticality",
    "short_description": "short_description",
    "vendor": "vendor",
    "equipment_model_entity_path": "equipment_model_entity_path",
    "first_discovered": "first_discovered",
    "hardware_version": "hardware_version",
    "status": "status",
    "backplane_name": "backplane_name",
    "backplane_id": "backplane_id",
    "slot_number": "slot_number",
    "rack_number": "rack_number",
    "module_type": "module_type",
    "device_type": "io_field_device_type",
    "support_group": "support_group",
    "site": "site",
    "ip_address": {
        "ip": "ip_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "mac_address": {
        "mac": "mac_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "memory": {
        "memory_card_serial": "memory_card_serial_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_size": "memory_size_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_type": "memory_type_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "software_installed": {
        "name": "software_installed_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "version": "software_version_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "install_date": "software_install_date_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    // Do not change this. Key should match value of SGOTAssetImportExcelConstants.CUSTOM_FIELDS_COL_NAME_IN_IMPORT_SET
    "custom_fields": {
        "customfield": "customfield_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    }
}

```

7. Select **Update** to save your changes.

8. Navigate to **All > Configuration > IntegrationHub ETL**.

9. Select the **CMDB Application: SG-OT Excel Import** ETL.

10. If the Invalid Mapping Data Detected page is displayed, select **Close**.

11. From the ETL Transform Map Assistant, in the Specify Basic Details section of the guided setup, select **Import Source Data and Provide Basic Details**.

SG-OT Asset Excel Import

ETL Transform Map Assistant

Use this guided walkthrough to create and manage ETL Transform Map for integrating third-party data into CMDB.

1. Specify Basic Details

Provide basic information for the ETL Transform Map.

Tasks

✓ Import Source Data and Provide Basic Details

12. In the Sample Import Set field, select Auto-pull a new import set.

Specify Basic Details

← Provide Basic Information for the ETL Transform Map

Save Mark as Complete

Unsaved Changes

Provide the template with some basic properties, and select a data source to map to CMDB.

* CMDB Application: SG-OT Excel Import

* Name: SG-OT Asset Excel Import

Description: ETL to import assets from Excel

* Data Source: SG-OT Excel Import

* Sample Import Set: Auto-pull a new import set

13. Select Save.

The basic information saved successfully banner is displayed.

14. Select Mark as Complete.**15. From the ETL Transform Map Assistant page, in the Prepare Source Data for Mapping section, select Preview and prepare data.**

now All Favorites History Workspaces IntegrationHub ETL

Search

Mark as Complete

Prepare Source Data for Mapping

Preview and Prepare Data

Nested Data Structure

New Transform Show data structure

object	status_value	support_group	support_group.sys_id	type	u_my_custom_field	vendor	vendor_cleaned	vendor_name_cleaned
object	get install status value	Original Value	get support group sys id	Original Value	My Custom value	Vendor E	cleanse vendor	Split - vendor_cleaned
object[1]				plc				48364f7453281110594addeeff7b127b Vendor E
								4836

If the column is not visible, repeat the steps 11 through 14.

16. Select Mark as Complete.**17. From the ETL Transform Map Assistant page, in the Map Data to CMDB and Add Relationships section, select CMDB Classes to Map Source Data.****18. Map the column to the target class and attribute.**

For example, the “comments” field is present on the Hardware `cmdb_ci_hardware` class. After this field is mapped, the “comment” field on Hardware child classes is updated as well, as long as the value for the “comments” column in the staging table for that row is not empty. If you’re adding a mapping for a new field that is not present, or for a field that is not specific to the Hardware `cmdb_ci_hardware` class, but instead is a field in the Operational Technology (`cmdb_ci_ot`) class, you would add the field mapping in the Operational Technology (OT) 1 stub.

a. Add a field mapping to the Hardware 1 class.

b. For the Hardware 1 class, select **Edit Mapping**.

Map Data to CMDB and Add Relationships
Select CMDB Classes to Map Source Data

Set target class to map your source data. To set specific rules for how source data should map to classes, add a conditional class.

Add Class Add Conditional Class

Basic Class

Hardware 1 cmdb_ci_hardware

Edit Class Edit Mapping

19. In the Add Attribute dialog box that appears, from the **Attribute** list, select **Comments**.

Map to Hardware 1

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data column

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

▼ Source Native Key ?

Source Column object>id ×

Add Attribute

Attribute Comments

comment

Comments ✓

Save

20. Select **Save**.

A new field named “Comments” is displayed. You may need to scroll to see the field.

Map to Hardware 1

Last Saved: 2021-10-28 13:29:49

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

Source Column object>model_number_id_cleansed ×

▼ Support group

Source Column object>support_group_sys_id ×

▼ Manufacturer

Source Column object>manufacturer_sys_id_cleansed ×

▼ First discovered

Source Column object>first_discovered_date_time_format ×

▼ Class

Source Column object>asset_cmdb_class_sys_name ×

▼ Comments

Source Column

21. From the Data pane, drag the data pill to the Comments **Source Column** field.

The screenshot shows the 'Map to CMDB Transform Data' page. In the 'Comments' section, there is a mapping configuration: 'Source Column' is 'object>u_my_custom_field' and 'Target Column' is 'Comments'. A red box highlights the 'Comments' target column. To the right, the 'Data' pane lists various CMDB attributes and their values, such as serial_number_cleaned (SN0001), serial_number_type (system), and type (plc). The 'Comments' row also shows its value as 'My Custom value'.

You can also select the source column icon () to select the data mapping field for it. The Source Column includes the data pill.

The screenshot shows the 'Map to CMDB Transform Data' page. In the 'Comments' section, there is a mapping configuration: 'Source Column' is 'object>u_my_custom_field' and 'Target Column' is 'Comments'. A red box highlights the 'object>u_my_custom_field' source column. The rest of the interface is similar to the previous screenshot, showing other mappings and the 'Data' pane.

22. Navigate back to the **CMDB Classes to Map Source Data** of the Map Data to CMDB and Add Relationships section in the ETL Transform Map Assistant page.

Map to Hardware 1
Last Saved: 2021-10-28 13:40:03

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

- Source Native Key** (object>id)
- Name** (object>name)
- Source Recency Timestamp**

23. Select **Mark as Complete.**

24. Follow these steps to verify the new field mappings.

- Navigate to the home page of the ETL Transform Map Assistant.
- In the Preview Sample Integration Results and Schedule Import section of the guided setup, select **Test and Rollback Integration Results**.

SG-OT Asset Excel Import

Delete Activate

ETL Transform Map Assistant

Use this guided walkthrough to create and manage ETL Transform Map for integrating third-party data into CMDB.

Tasks

2. Prepare Source Data for Mapping

Preview the third-party source data, and prepare it for mapping to CMDB classes and attributes.

✓ Preview and Prepare Data

Tasks

3. Map Data to CMDB and Add Relationships

Choose target classes in the CMDB to map source data to, and add any relationships amongst these classes.

✓ Select CMDB Classes to Map Source Data

✓ Add Relationships

Tasks

4. Preview Sample Integration Results and Schedule Import

Run your ETL Transform Map, make any necessary adjustments and perform rollback if needed.

✓ Test and Rollback Integration Results

Set Import Schedule

c. Select **Run Integration.**

- After the run finishes successfully, confirm that the Comments field of the CI that you provided a comments value for is updated in the staging table.

e. Select **Mark as Complete.**

f. Select Perform Rollback.

g. If the ETL is not activated, select **Activate**.

The new column field mapping is successfully added and verified.

Add a custom implementation for device classification

Customize the base system classification of an device based on the type, os_version, and firmware_version.

Before you begin

The base system for the `sn_otsm_sgc.SGOTAssetImportExtensionPoint` extension point uses the default implementation script that is shipped with the name of `sn_otsm_sgc.SGOTAssetImportUtil`. To add a customized classification, create an implementation for the extension point in the **Service Graph Connector for Operational Technology (Excel)** scope.

- i Note:** User must have only one implementation of the extension point. If you implement and activate a custom extension point rather than the default one, you must deactivate the default implementation.

Role required: cmdb_inst_admin, import_admin, import_scheduler, admin

Procedure

1. Navigate to **All > System Extension Point > Scripted Extension points**.
2. Select `sn_otsm_sgc.SGOTAssetImportExtensionPoint`.
3. Select the **Create Implementation** related link.

4. Enter a name for the extension point implementation.
5. In the script field, check that the class object with the following two functions is populated. Make sure that the result returned from the **getAssetCMDBSysClassNameWithOtEntityTypeSysId** extension point follows the format mentioned in the comments. Any change in the result string format results in import failure or irregularities. The format should be <cmdb class name>:::<ot entity type sys id>.

Option	Description
<pre>getAssetCMDBSysClassNameWithOtEntityType- SysId(/*string*/ type, /*string*/ osVersion, /*string*/ firmwareVersion)</pre>	<p>Implement this method to return the CMDB sys class name that the device belongs to, along with the OT Entity type sys_id concatenated with "...".</p> <p>For unclassified devices, the OT device type is set to ot_base.</p>
<pre>getComputerType((/*string*/ operatingSystem)</pre>	<p>Returns the CMDB sys class name based on the operating system passed.</p>

6. After you make all the desired changes, select **Update**.
The implementation for the extension point is created.

What to do next

From the related lists Implementations tab, open the base system extension point implementation to deactivate it.

Add a custom validation for devices

Customize the validation for your OT devices.

Before you begin

The base system for the **sn_otsm_sgc.SGOTAssetCustomValidationExtensionPoint** extension point uses the default **sn_otsm_sgc.SGOTExcelStagingAssetValidationProcessor** implementation script. You can add a customized validation by creating an implementation for the extension point in the Service Graph Connector for Operational Technology (Excel) scope.

Role required: cmdb_inst_admin, admin

Procedure

1. Navigate to **All > System Extensions Point > Scripted Extension Points**.
2. Select **sn_otsm_sgc.SGOTAssetCustomValidationExtensionPoint**.
3. Select the **Create Implementation** related link.
A script include is created where you can add your custom validation.

4. To add a custom validation, refer to the following validation

A	B	C	D	E	F	G	H	I	J
Custom Validation	Invalid (Override - False)	Valid (Override - False)	Partially Valid (Override - False)	Invalid (Override - True)	Valid (Override - True)	Partially Valid (Override - True)	No Implementation created (Override - True)	Implementation has different Name (Override - True)	Invalid state (Type) (Override - True)
Default Validation	Partially Valid								
2 (en_otm_sg.enable.cmdb.validations - True)	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
3 (en_otm_sg.enable.cmdb.validations - True)	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
4 (en_otm_sg.enable.cmdb.validations - True)	Invalid	invalid	invalid	invalid	invalid	invalid	Invalid	Invalid	Same as Default state
5 (en_otm_sg.enable.cmdb.validations - False)	Partially Valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
5 (en_otm_sg.enable.cmdb.validations - False)	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
7 (en_otm_sg.enable.cmdb.validations - False)	invalid	invalid	invalid	invalid	invalid	invalid	Invalid	Invalid	Same as Default state

scenario.

5. Select **Update**.

Test the Excel Service Graph connector

The troubleshooting actions can help resolve common issues when importing your Operational Technology devices or data. Access the System Log to troubleshoot for these errors.

These logs can be used to debug any issues or to find the SGC steps are executed properly.

Issue	Solution
If there is an issue while loading data for SG-OT Device Excel Import ETL on ETL guided setup	<p>From the Related links list, try loading the data.</p> <ol style="list-style-type: none"> 1. Navigate to the SG-OT Excel Import data source and select Test Load 20 Records or Load All Records. 2. Return to ETL and try loading the data again.
If there are entries in the Partial payload tab after test running the Service Graph connector from ETL guided setup	<p>Due to the following conditions:</p> <ul style="list-style-type: none"> • Missing values for the required fields of an device. • Control Modules without a parent device associated with it - Check that the type of the device and control module parent id field is filled properly in the staging table.
If there are entries in the Incomplete payload tab after test running the Service Graph connector from ETL guided setup	<p>Due to the missing values for fields that are used uniquely to identify an device.</p>
After easy import is executed, users may see records that are imported from the current run. When validations are executed, they are run on all records of the staging table not only on records from the current import run.	<p>Before running the validations, the user must click ALL on the list view breadcrumb of the staging table.</p>
If the timestamp column appears empty on the staging table	<p>The user must use the UTC format (YYYY-MM-DD hh:mm:ss) to enter the date and time.</p>
If the validation state update on records is not visible after click Run Validations button.	<p>The user must manually refresh the page.</p>

Issue	Solution
<p>When the user changes the existing data of the records in the staging table, the validation state is not set to Pending Validation.</p>	<p>The validation state is set to Pending validation, when the following attributes are changed:</p> <ul style="list-style-type: none"> • Identifier fields (Mac-address (1-9)) • Serial Number • Name • Correlation ID • Type • Control module parent correlation ID • Fields used in transformed name computation • Rack Number • Slot Number <p>For more information about the system properties, see System properties that impact SG-OT Device Excel Import processing.</p>
<p>After records are imported into the staging table, the updates done in the system properties related to transformed name computation are not reflected in the staging table records.</p>	<p>Change the system properties before importing the data into the staging table.</p>
<p>If the multiple error banners are shown when users select few records and click Run Validation.</p>	<p>The validations are executed for all the records available in the staging table.</p> <p>Do not select the single record for validation.</p>
<p>If the duplicate records exist in CMDB, the staging table does not detect it as duplicate.</p>	<p>The validations are executed only for the data available in the staging table.</p> <p>The validations are not executed for the data available CMDB.</p>
<p>The site name is provided in the spreadsheet or staging table, but not shown on the OT devices after the import of the spreadsheet.</p>	<p>Only the existing site records in the CMDB are considered.</p> <p>The entity_name for the site (ISA Equipment model entity) must match the value provided in the site column in the excel or staging table.</p> <p>If the entity_name for the site does not match, the value is set to empty.</p>
<p>When users click Load All the records on the data source, no records are imported into the import set.</p>	<p>No records are available in the staging table.</p>

Issue	Solution
	<p>The records are present in the staging table, but the records are not in Valid or Partially valid state.</p> <p>Access all the logs related to Excel SGC in All > System logs > System log > All. Search for the string SGOTExcel in the Message column.</p>

View script includes used by the Service Graph Connector

As an admin, view the script includes related to the Service Graph Connector.

Before you begin

View a filtered list of all the scripts that are used by the Service Graph Connector.

Role required: cmdb_ot_admin, cmdb_inst_admin, or admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager > Import OT Devices - Script Includes**.

This list shows the records whose names begin with SGOTAsset or SGOTExcelStaging.

2. View the list of scripts.

Access system properties used by the Service Graph Connector

As an admin, view system properties related to the Service Graph Connector.

Before you begin

View a filtered list of all the scripts that are used by the Service Graph Connector.

Role required: admin, cmdb_inst_admin, or cmdb_ot_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager Admin > Import OT Devices - System Properties**.

The list shows records whose names begin with **sn_otsm_sgc.excel**.

2. View the list of scripts.

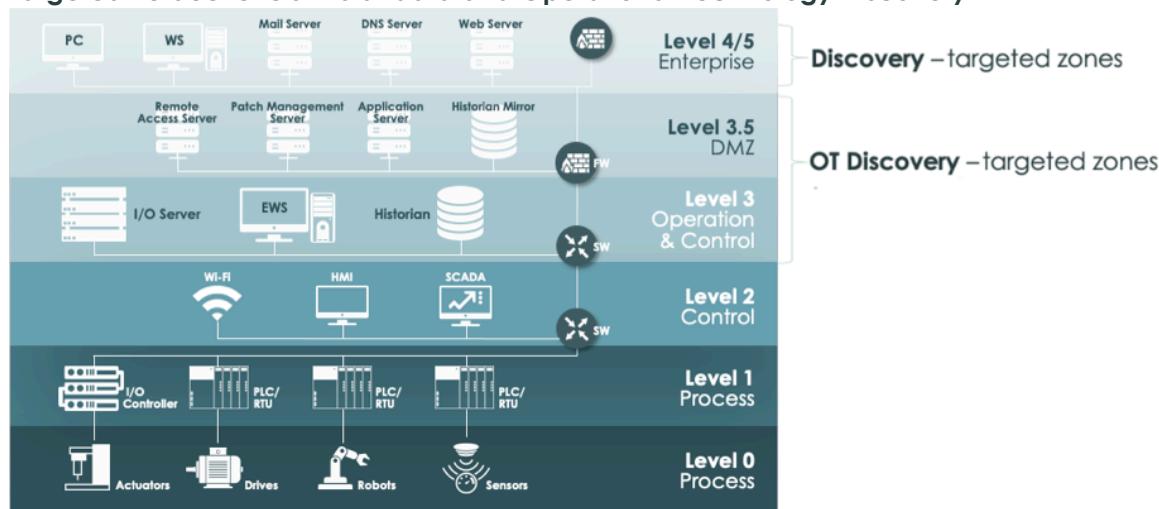
Discovery for Operational Technology

You can run the Discovery for Operational Technology function to discover IT class Operational Technology (OT) devices in designated Purdue levels in your Industrial Control System (ICS) networks. IT class items include switches, routers, and computers that exist both in data centers and in your factories.

Where standard Discovery processing takes place

The Discovery for Operational Technology process operates in a manner that is similar to the standard Discovery processes.

Targeted Purdue levels in standard and Operational Technology Discovery



Standard Discovery processing in the Now Platform[®] normally takes place in the following Purdue levels in your enterprise:

Processed Purdue levels

Purdue Level	Description
4	Site business and logistics, such as all Information Technology (IT) functions.
5	Enterprise Network, where Enterprise Resource Planning (ERP) functions take place.

Note: To learn more about Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.

Where and how Discovery for Operational Technology processing takes place

In contrast, Discovery for Operational Technology processing can take place in the following Purdue levels, depending on which you select when you create an OT discovery schedule:

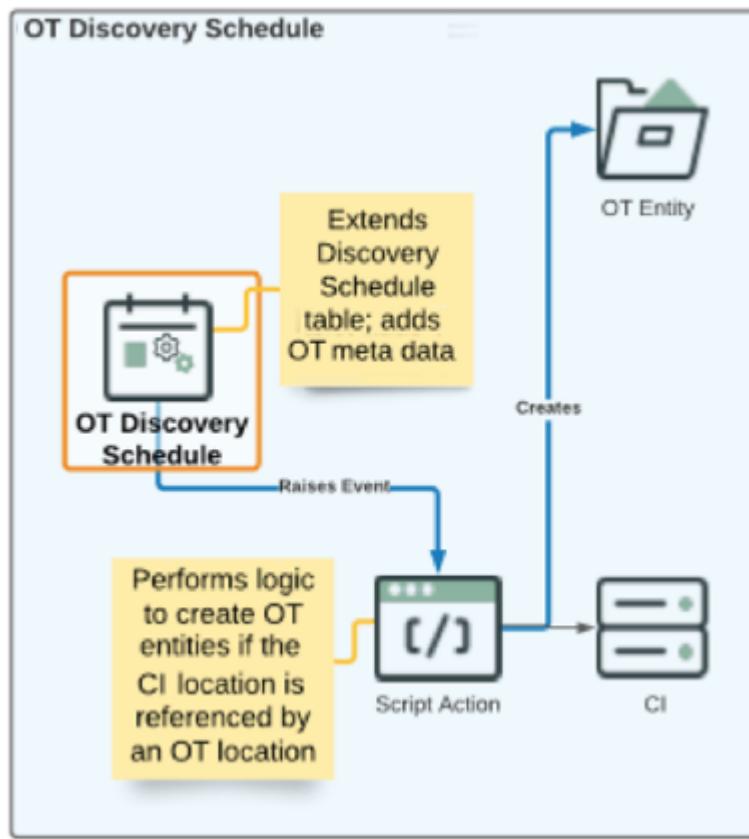
Processed Purdue levels

Purdue Level	Description
3.5	Demilitarized Zone (DMZ) or Industrial Demilitarized Zone (IDMZ). Similar to a traditional (IT) DMZ, the OT-oriented IDMZ enables you to securely connect networks with different security requirements.
3	Site operations where plant or site-wide control and monitoring functions reside.

You typically run Discovery for Operational Technology in the DMZ (or IDMZ, Purdue Level 3.5) of your ICS networks. This Purdue level is where there are usually IT and OT class computers and servers to discover and manage.

Note: To avoid the possibility of disrupting your industrial operations, you should not run Discovery processes against Purdue levels 0 through 2 in your ICS networks.

Discovery for Operational Technology processing



When you run an OT discovery schedule, it performs the following processing:

1. Proceeds through the assigned IP addresses and discovers all hardware items that exist in it.
2. When it completes discovery of a configuration item (CI), it internally triggers a (discovery.device.complete) event. This logic checks if an OT entity (cmdb_ot_entity) record exists for it in the Configuration Management Database (CMDB).
 - If one exists, and any related attributes have changed for the discovered item, it updates the OT Entities that are related to that CI.
 - If one does not exist, it creates one for it.
3. In addition to the location attribute, it also pushes the defined attributes from the OT discovery schedule to the CI and to the related OT entity records.
4. It also creates OT entity records for the applications installed on discovered OT devices. To view the applications that have OT entity records created through OT Discovery, navigate to the Industrial Workspace list view and open the **Applications** list under **Operational Technology (OT)**.

Related topics

[Operation Technology \(OT\) extension classes](#)

[MID Server](#)

[Discovery](#)

Horizontal discovery process flow with probes and sensors [↗](#)

Schedule a horizontal discovery [↗](#)

Discovery for Operational Technology related links and lists

Discovery for Operational Technology contains several related links and lists.

Related links

Related link	Description
Quick Ranges	IP addresses and address ranges to scan when the OT discovery schedule runs. Enter IP addresses in multiple formats (network, range, or list) in a single, comma-delimited string. The MID server in use must be able to connect to the specified IP ranges. For more information, see Create a Quick IP range for a Discovery schedule ↗ .
Discovery now	Run the Discovery for Operational Technology process immediately.
Run Point Scan	Access to the Execute Point Scan dialog. To learn more, see Execute a point scan ↗ .

Related lists

Related list	Description
Discovery IP Ranges	Discovery IP addresses and address ranges to scan and discover. If you are using a simple CI scan (no behaviors), use this related list to define these IP addresses. The MID server in use must be able to connect to the specified IP ranges. i Note: To improve security, limit the range of discovery targets to exclude unnecessary networks and devices.
Discovery Range Sets	Definition of each range set that the OT discovery schedule scans, using one or more Shazzam probes.
Discovery Status	History of the results of the current and past OT discovery schedule runs.

Related topics

[MID Server](#) [↗](#)

[Shazzam probe, port probes, and protocols](#) [↗](#)

[Create a Shazzam probe](#) [↗](#)

Create an Operational Technology discovery schedule and run the Discovery process

Define Operational Technology (OT) discovery schedules that orchestrate how and when the Discovery for an OT function should run. You can also perform an immediate Quick Discovery or an actual OT Discovery run.

Before you begin

Do the following actions before you run Discovery for Operational Technology:

- Install and configure the standard Discovery application. To learn more, see [Discovery setup](#).
- Install the CMDB CI Class Models plugin. To learn more, see [Operational Technology \(OT\) extension classes installation](#).
- Install the Mid Server. To learn more, see [Installing the MID Server](#).

Role required: ot_discovery_admin

Procedure

1. Navigate to **All > OT Discovery > OT Discovery Schedules**.
2. Run Quick Discovery, or select or create an OT discovery schedule.

Task	Description
Run an immediate Quick Discovery	<p>Click Quick Discovery and do the following actions:</p> <ol style="list-style-type: none"> In the Target IP field, enter the IP address in which the Discovery for the OT process should run. In the MID Server field, select the MID Server in which the Discovery process should run. Click OK.
Select or create an OT discover schedule	<ol style="list-style-type: none"> Select an existing OT discovery schedule or click New to create a new one. Perform the steps that follow to create the OT discovery schedule record in the OT Discovery Schedule form.

3. In the form, fill in the OT Discovery Schedule fields.

Field	Description
Name	Unique, descriptive name for your OT discovery schedule.
Discover	<p>Scan type for the OT discovery schedule.</p> <p>Configuration items</p> <p>Uses Discovery identifiers to match devices with configuration items (CIs) in the CMDB and to update the CMDB. Perform a simple discovery by selecting a specific MID Server to scan for all protocols (SSH, WMI, and SNMP) or perform advanced discoveries with discovery behaviors. When you select a behavior, the MID Server field is not available.</p>
	IP addresses

Field	Description
	Scans devices without the use of credentials. These scans discover all the active IP addresses in the specified range and create device history records, but do not update the CMDB. IP address scans also show multiple IP addresses that are running on a single device. Identify devices by class and by type, such as Windows computers and Cisco network gear.
Default Purdue level	Purdue level that you want the OT discovery schedule to run in, or select --None-- for all Purdue levels. i Note: To learn more about Purdue levels, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model      

Most of the fields on this form are identical to or operate in the same manner as the standard Discovery form. Only those fields that differ from the standard Discovery scheduling appear in this topic. To learn more about the remaining fields, see [Schedule a horizontal discovery](#)

- Run the Discovery process right away, or save the OT discovery schedule to run at the times you designated in the record.

Task	Description
Run Discovery immediately	Click the Discover now related link.
Run Discovery at the time designated in the OT discovery schedule	Click Update .

Result

When the Discovery for Operational Technology process runs, it creates a history record in the Discovery Status related list.

Edit or view OT devices after import or discovery

Use the options on the Operational Technology (OT) menu to edit or view detailed information for the OT devices in your enterprise.

Before you begin

Import your Operational Technology device data in any of the following ways:

- Use the Microsoft Excel spreadsheet template with the Integration Hub Extract Transform Load (ETL), an Operational Technology certified Service Graph Connector. For more information, see [Import your Microsoft Excel spreadsheet using the staging table](#).
- Run Discovery for Operational Technology. For more information, see [Discovery for Operational Technology](#).
- Use an Operational Technology Certified Service Graph Connector from the ServiceNow Store.

Role required: cmdb_ot_viewer, cmdb_ot_editor, cmdb_ot_admin, or admin

About this task

If you have an assigned cmdb_ot_viewer role, you can only view OT devices. If you have an assigned cmdb_ot_editor or cmdb_ot_admin role, you can edit OT device records in the following ways:

- Edit OT device records individually on the Now Platform.
- Bulk edit multiple OT device records from the Industrial Workspace list view.

Procedure

1. To edit one OT device record Now Platform, follow these steps.

- a.** Navigate to **All > Operational Technology (OT)** and select one of the following menu items:

All OT Devices

By default, this list does not include control modules.

All OT Devices by IP Address

When you view the All OT Devices by IP Address list, note the following:

- An OT device with multiple IP addresses is displayed once per assigned IP address.
- Select the name of the OT device to open the OT device record. Selecting the IP address that is displayed for the record opens the record of only the IP address.
- You **cannot** create a new OT device record from this list.

OT Control Systems

By default, this list does not include control modules.

OT Control Systems with Modules

When you view the OT Control Systems with Modules list, note the following:

- The list view displays all the Control Modules grouped by their parent Control System.
- You cannot create a new OT device record from this list.

- b.** In the **OT device** column, select the OT device that you want to edit.

- c.** On the form, fill in the fields.

- d.** Click **Update**.

2. To bulk edit multiple OT device records Industrial Workspace, follow these steps.

a. Navigate to **All > Industrial Workspace**.

b. Open the list ( view and select one of the following lists available under **Operational Technology (OT)**.

- OT Supervisory Systems
- OT Control Systems
- OT Field Devices
- OT Computer and Servers
- OT Network Gear
- Industrial IoT (IIoT)
- Unclassed OT Devices

c. Select the check box next to each OT device that you want to edit.

Note: You can only bulk edit OT devices with the same **Class** field. You can't use the bulk edit feature for OT devices with different classes.

d. To edit the configuration item (CI) fields, select the **Edit** button and edit the form fields as needed.



A screenshot of a ServiceNow list page titled "OT Supervisory Systems" with 24 items. The page includes standard list controls like refresh, search, and export, followed by a toolbar with icons for create, edit, delete, and search. A red box highlights the "Edit (7)" button, which is part of a dropdown menu. Below the toolbar, there is a note indicating the last refresh was 21m ago.

Note: The maximum number of records that you can bulk edit the CI fields for is the records shown on a single page.

e. Click **Update**.

f. To edit the OT device details, select the **Edit OT details** button and edit the form fields as needed.



A screenshot of the same "OT Supervisory Systems" list page. The toolbar now includes an additional button labeled "Edit OT details (7)", which is highlighted with a red box. The note below the toolbar indicates the last refresh was 22m ago.

Note: Bulk editing OT details is a background job that can take time to complete. If the background job is busy, you can't bulk edit other OT device records.

OT device related items and related lists

The All OT Devices, All OT Devices by IP Address, and All OT Devices by CI menu options contain several related items and lists.

Related items

This section lists any related or subordinate items that are associated with this OT device.

Note: Not all OT devices display the following related lists. For OT devices in an Operational Technology class or extended class, the following related lists are displayed. For OT devices categorized in a different hardware class, such as Windows Server, an instance admin must add the related lists to the form.

1. To view the related records, click the name of the related item (for example, Memory Modules).
2. To add a configuration item (CI) relationship for this OT device, click the add CI relationships icon (+). Use the search field to find the CI item that you want to create a relationship for.
3. To access the Dependency View form to see a pictorial depiction of the OT device relationships, click the show dependency views icon ().
4. To change the settings that govern how the related items appear and are filtered, click the settings icon ().

OT device related lists

Related list	Description
Equipment Model Entities	The equipment model entities that are automated by the OT device.
Network Adapters	The names, MAC addresses, IP addresses, Netmasks, MAC manufacturers, and Dynamic Host Configuration Protocol (DHCP)-enabled indicators. It includes statuses of the network adapters that are associated with the OT device.
Serial Numbers	The serial numbers, validity indicators, and serial number types that are associated with the OT device.
Memory Modules	The serial numbers, validity indicators, and serial number types for the memory modules that are associated with the OT device.
Software Installed	The application software, if any, that is installed for the OT device.
IP Address	The IP addresses, IP versions, Net masks, NIC numbers, and configuration items that are associated with the OT device.
OT Incidents	The OT incidents that are associated with the OT device.
OT Change Requests	The OT Change requests that are associated with the OT device.
OT Vulnerable Items	The vulnerable items that are associated with the OT device.
OT Control Modules	<p>The control modules that are associated with the OT device of type OT control system or extended classes (for example, PLC).</p> <p>Each OT control module that has an "Owned by: Owns" relationship with the OT Control System record that is displayed.</p> <p>In the platform, the user can create an OT Control module.</p> <p>You can choose from the following Input/Output values depending on the Module type field:</p>

OT device related lists (continued)

Related list	Description
	<ul style="list-style-type: none"> • None • Local • Remote • Distributed
External System Metadata	<p>The URL of the device in the source system, discovery source, and updated devices that are associated with the CI.</p> <p>The URL is automatically populated by the source system through the service graph connector.</p>
OT Protocols	<p>This is applicable for protocol converter class.</p> <p>The protocols, description, vendor, and version that are associated with the protocol converter class.</p>

Operational Technology device form

Use the Operational Technology (OT) device form to edit the detailed information for the OT devices in your enterprise.

Operational Technology device form

Field	Description
OT display name	<p>The name of the OT device displayed in the record.</p> <p>i Note: You can add any string value to this field. Multiple devices can have the same OT display name. This is meant for easier understanding of the OT device and is different from the unique CI name generated when you import OT devices from the staging table.</p>
OT device type	<p>The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example:</p> <p>An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is server and its device type is HMI.</p>

Operational Technology device form (continued)

Field	Description
	<p>i Note: In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select No OT Function. For OT devices where the device type is unknown, select Unknown.</p>
Device criticality	<p>The measure of the relative risk to the site process of failure of the device. For example:</p> <ul style="list-style-type: none"> • 1 - Most critical • 4 - Not critical
Site	<p>The top-level parent entity, or industrial site, where the device is located or assigned to.</p>
Purdue level	<p>The assigned Purdue level. Ranges 0–5.</p> <p>i Note: To learn more about Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.</p>
Zone	<p>The area within the site location that the device is assigned to.</p>
Class	<p>The name of the assigned class for the OT device.</p> <p>i Note: For a listing and explanation of CI classes, see Operation Technology (OT) extension classes.</p>
Status	<p>Status of the OT device:</p> <ul style="list-style-type: none"> --None-- No assigned status. Absent OT device is absent in your facilities. In Maintenance OT device is in maintenance and currently is off line. In stock OT device is in stock in your facilities.

Operational Technology device form (continued)

Field	Description
	<p>Installed OT device is installed in your facilities.</p> <p>Pending Install OT device is pending installation in your facilities.</p> <p>Pending repair OT device is pending repair but is not online yet.</p> <p>Retired OT device is retired.</p> <p>Stolen OT device has been stolen.</p>
Discovery source	The Discovery source for the OT device data. For example, SG-OT Excel Import, if you imported the OT device from a Microsoft Excel spreadsheet using the Integration Hub ETL. To learn more, see Service Graph Connector for Operational Technology (Excel) .
Infrastructure Relationships	Shows the relationship of OT device with other the OT devices and the equipment model entities.
Service Relationships	Shows the relationship of OT device with the equipment model entities.
CI Timeline	Shows the timeline of OT incidents, OT change, and audit history associated with the OT device.
The following fields only apply to the Programmable Logic Controller (PLC) Class Records:	
Key switch	<p>The Key switch modes:</p> <p>Remote mode You can change the configuration of the PLC.</p> <p>Local mode By default mode, you can't change the configuration of the PLC.</p>
Switch position	<p>The Switch position of the PLC has the following positions:</p> <ul style="list-style-type: none"> • Run • Program • Remote

Operational Technology device form (continued)

Field	Description
	<ul style="list-style-type: none"> • Stop • Test <p>By default, the switch position is set to None. When the switch position is set to Remote, the Switch remote modes are enabled.</p>
Switch remote mode	<p>The Switch remote of the PLC has the following modes:</p> <ul style="list-style-type: none"> • Run • Program • Test • None

Create the OT Protocol

OT protocols table helps users to capture the information related to protocols such as name, version, it is a vendor-specific protocol or not. The protocols are the medium of communication between the different devices connected to the Industrial network.

Before you begin

Role required: OT_admin and admin

Procedure

1. Navigate to **All > Operational Technology (OT) > OT Protocols**.
2. On the OT Protocols page, click **New**.
3. Fill in the fields on the OT Protocol form.
4. If the protocol is vendor-specific protocol, select the **Vendor specific** check box.
5. Click **Submit**.

Map OT protocols to protocol converter CIs

Relate Operational Technology (OT) protocols to protocol converter configuration items (CI) in the Industrial Workspace.

Before you begin

Role required: cmdb_ot_editor

Procedure

1. Navigate to **All > Industrial Workspace** and open the Industrial Workspace list view.
2. In the **All OT Devices** list, select a Protocol Converter record.
3. In the record, select the **Related Records** tab.
4. Select the OT Protocols related list.
5. Select **Add**.

6. Select the protocols that you want to add to the protocol converter record and click **Add**.
The protocols are added to the related list.
7. Optional: To remove protocol records from the related list, select the records you want to remove and click on **Remove**.

Convert an IT hardware device to an OT device

If you've identified IT hardware devices that belong to the OT network, you can convert these IT Configuration Items (CI) into OT devices.

Before you begin

Role required: cmdb_ot_admin or admin

About this task

This task is applicable to all IT hardware devices.

Procedure

1. Select an IT CI.
For example, you can navigate to **All > Configuration > Base Items > Computers**.
2. Select the IT hardware device that you want to convert to an OT device.
3. In the Related Links module, select **Add OT Device Details**.

The OT Device form is displayed.
4. Fill in the fields on the OT Device details form.
5. Select **Update**.
6. To view the converted OT Device, navigate to **All > Operational Technology (OT) > All OT Devices**.

Result

The selected IT hardware device has been converted to an OT device.

Alternatively, you can select multiple IT hardware devices and convert them into OT devices in a bulk edit. For more information, see [Convert IT hardware to OT devices in a bulk edit](#).

Convert IT hardware to OT devices in a bulk edit

Choose multiple IT hardware devices and convert them to OT devices in a bulk edit so that you can edit your records more quickly and efficiently.

Before you begin

Role required: cmdb_ot_admin or admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Workspace**.
2. In the Industrial Workspace, navigate to the All IT Hardware list.
3. Optional: If you want to filter the All IT Hardware list, do the following actions:
 - Select the filter  icon in the top-right corner of the list.
 - Add the filter that you want applied to the list.
 - Select **Update**.
4. Select the check box next to each of the IT hardware devices that you want to convert.

If you want to select all IT hardware devices in the list, select the check box next to the Name column.

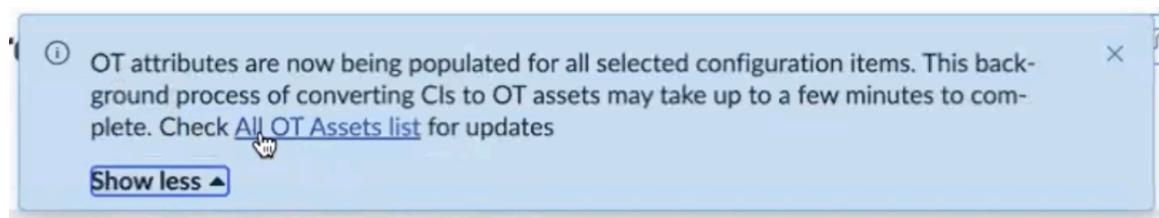
5. Select the **Convert to OT devices** button.
6. On the form, fill in the fields.

Convert to OT devices form

Field	Description
OT Device Type	<p>The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example:</p> <p>An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is server and its device type is HMI.</p> <p>i Note: In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select No OT Function. For OT devices where the device type is unknown, select Unknown.</p>
Device Criticality	<p>Measure of the relative risk to the site process if the device fails:</p> <ul style="list-style-type: none"> ◦ 1 - Most critical ◦ 4 - Not critical
Purdue Level	<p>Assigned Purdue level. The level ranges are 0–5.</p> <p>i Note: To learn more about the Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.</p>
Zone	area within the site location that the device is assigned to.
Site	Top-level parent entity, or industrial site, where the device is located or assigned to.

7. Select **Convert**.

The following banner appears to let you know the process has started. To check the All OT Devices list for updates, you can select the link in the banner.



Result

The selected IT hardware devices have been converted into OT devices.

You can also use the Bulk Update Ruleset for Reassigning IT to OT feature to create a scheduled job that automatically converts IT hardware to OT devices. For more information, see [Automatically convert your IT records to OT devices](#).

Convert your OT devices to IT hardware devices in a bulk edit

Bulk edit your Operational Technology (OT) devices to remove the OT device details. Then convert your OT devices to IT hardware devices.

Before you begin

Role required: cmdb_ot_admin or admin

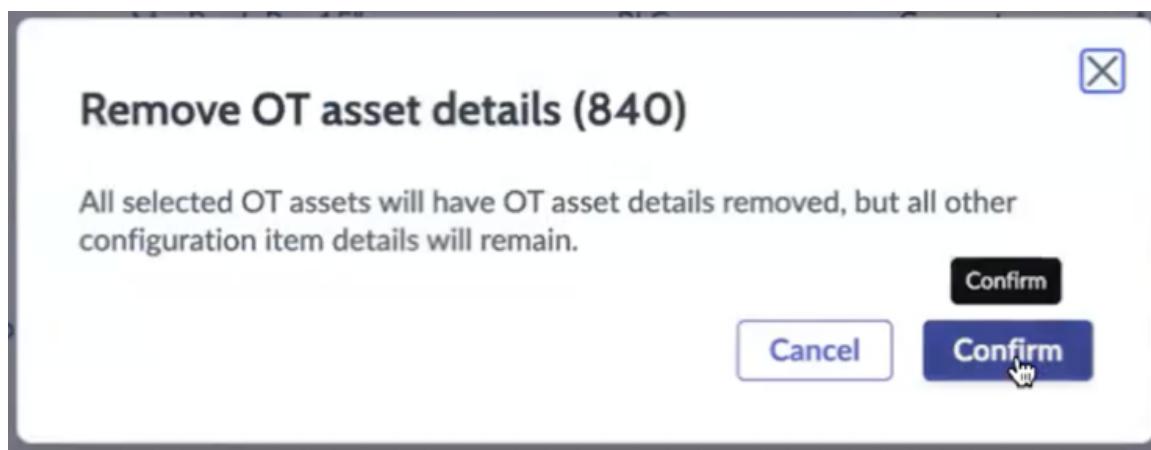
About this task

If you encounter OT devices that don't have an OT function and should be classified as IT hardware devices, you can select and edit multiple OT devices in a bulk edit to convert them to IT hardware devices.

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Workspace**.
2. Navigate to the All OT Devices list view in the Industrial Workspace.
3. Select the OT devices that you want to convert to IT hardware devices.
If you want to select all OT devices in the list, select the check box next to the OT device column.
4. Select the **Remove OT device details** button.
A dialog box appears that asks you to confirm that you want to remove the OT device details but keep all the other configuration item details.

Note: None of the CI details, network adapters, or IP addresses are removed. Only the OT-specific data is removed.



5. Select **Confirm**.

Result

The OT device details are removed from the selected OT devices and the OT devices are converted to IT hardware devices. You can view these IT hardware devices in the IT Hardware list view on the Industrial Workspace.

Managing Network Intrusion Detection System appliances

If you have the cmdb_nids_admin or admin role, you can assign metadata attributes to Network Intrusion Detection System (NIDS) class records from the NIDS menu in the Now Platform.

A Network Intrusion Detection System helps manage the import of IT and OT devices from supported integrations. Assigning meta data such as location and NIDS network type to NIDS records helps you distinguish between detected OT and IT devices, and automatically adds the related meta data to the created records. Users with the cmdb_nids_admin or admin role can edit the **NIDS Assigned Meta Data** tab and view the changes made by the user in the Activity Stream.

Note: Manual creation for an NIDS record in the table is restricted from the list view or the form view of the records.

For more information about the NIDS class records, see [Network Intrusion Detection System \(NIDS\) CI extension class](#).

If a NIDS record has the Validated field set to true, then when any of the following attributes of the NIDS are changed on the NIDS form, a warning message is displayed.

- NIDS network type
- NIDS source name
- NIDS source ID

If the NIDS record with any detects::detected by relationships is deleted, a warning message is displayed.

You can use the Network Intrusion Detection Systems (NIDS) Guided Setup to lead you through:

- Configuring users and roles for users that do not already have an account in an instance
- Importing NIDS records from Operational Technology (OT) Certified Service Graph Connectors to designate if NIDS appliances are running on OT or IT networks
- Validating NIDS so that detected devices can be imported. For more information about validating NIDS, see [Validate the NIDS](#).

To access the NIDS Guided Setup, navigate to **Network Intrusion Detection Systems (NIDS) > NIDS Guided Setup**.

To assign an appliance as a manager for NIDS sensors that detect devices, navigate to **Network Intrusion Detection Systems (NIDS) > Managers** to edit applicable "management consoles" or "central managers" records.

- Review the Sensors list to ensure that there is not currently a device assigned as manager.
- For any devices that do not function as sensors, change **is manager** to **True**.

For information about the `NIDSUTILS` script include that copies NIDS-assigned meta data to detected devices, see [Script includes installed with Operational Technology Manager](#).

Related topics

[Network Intrusion Detection System \(NIDS\) CI extension class](#)

[Script includes installed with Operational Technology Manager](#)

Validate the NIDS

Validate the NIDS to import the devices from the ETL that were detected by the sensor. The sensors can only pass the validation if they aren't in learning mode as such sensors aren't eligible for device import.

Before you begin

It's recommended that you have the Common Service Data Model plugin installed. The Service Graph Connector aligns with the life cycle data models as per the Configuration Management Database (CMDB) standards. For more information, see [Implementing the CSDM framework in stages](#).

Role required: `cmdb_nids_admin`

About this task

The **Life Cycle Stage** and **Life Cycle Stage Status** fields are used to capture the learning mode of a sensor. If the Life Cycle Stage field is set to **Operational** and Life Cycle Stage Status is set to **Learning Mode**, then validation is unsuccessful. If the Life Cycle Stage Status field is set to **In Use**, the validation is successful.

Procedure

1. Navigate to **All > Network IDS Appliance (NIDS) > Sensors**.
2. If there are any management consoles or central managers in the list, do the following actions:
 - a. Click **edit the record**.
 - b. In the **NIDS Admin Configuration** tab, select **Is NIDS manager** to set the **Validated** column true.
3. In the NIDS Admin Configuration section, make sure that the **Life Cycle Stage Status** value is not Learning Mode.
Otherwise, the validation fails.

4. Select the **NIDS network type**.

The Network type must be selected based on the location of the sensor.

Note: The network type OT creates the OT device record. The network type IT does not create the OT device records.

5. In the **NIDS Assigned Meta Data** tab, check that all the devices discovered by the NIDS are entered.

6. Click **Validate**.

Note:

The zone value is populated by the ETL. If a zone value is manually entered on the NIDS record, it is overridden what is populated by the ETL.

If the NIDS record is not validated, the devices are not imported from the ETL that were detected by the sensor.

Automatically convert your IT records to OT devices

Create a scheduled job that automatically converts your IT hardware to Operational Technology (OT) devices by using the Bulk Update Ruleset for Reassigning IT to OT feature. This scheduled job adds OT entity details to all the IT hardware that you want to convert at once.

Before you begin

Role required: admin

About this task

You may have configuration items (CIs) classed as IT hardware that you want to create OT entity records for. Follow these general guidelines:

- Make sure that the fields you use apply to the filter criteria conditions in steps 3 to 4. Verify that the data set doesn't exceed 1 million records so that you can avoid performance-related issues.
- Create separate scheduled job definitions for the separate CI classes in steps 3 to 6. This way, you can filter each CI level and define the OT entity default values.
- Use the Class field in the filter to query only specific CI classes in step 3.

Note: Only the hardware class and its extended classes are used in the source table.

- Use the **Preview** button to verify the records selected for further review in step 4.
- Verify the data in the **OT Entity Default Configuration** tab in step 5. The OT entity records are created using these default values.

You can also manually convert the IT hardware to the OT devices. For more information, see [Convert IT hardware to OT devices in a bulk edit](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > OT Manager Admin > Automated IT OT Bulk Conversion**.
2. Select **New**.

3. On the **Filter Criteria - OT Devices** tab, set the source table and filter criteria to identify the CIs that you need to convert.

For example, if you want to add the OT entity details for all computers that are imported into the system that have a prefix of COMP, select the source table as **cmdb_ci_computer** and then add the filter criteria as **[Name] [starts with] [COMP]**, **[Class] [is] [Computer]**, and **[OT device details] [is empty]**.

The screenshot shows the 'Filter Criteria - OT Devices' interface. At the top, there are tabs for 'Filter Criteria - OT Devices', 'OT Entity Default Configuration', and 'Execution Details'. The 'Filter Criteria' tab is selected. Below it, the 'Table' dropdown is set to 'Computer [cmdb_ci_computer]'. Under 'Filter Criteria', the 'Preview' button is highlighted. The filter conditions are defined as follows:

- All of these conditions must be met:**
 - Name** starts with **COMP**
 - Class** is **Computer**
 - OT device details** is **empty**
- or**
- New Criteria**

empty].

4. Verify the number of records that were chosen from the filter condition you set by selecting the **Preview** button.

The OT entity details are added for these records, such as OT Device Type and Device Criticality.

5. On the **OT Entity Default Configuration** tab, fill in the fields.

The fields in the following table provide the default values that are added to the OT entity records or the OT-related metadata.

OT Entity Default Configuration form

Field	Description
OT Device Type	<p>Category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example, an IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Its class is server and its device type is HMI.</p> <p>i Note: In some cases, OT devices have no OT function or the device type is unknown. Where the OT devices have no OT function, select No OT Function. Where the OT devices have an unknown device type, select Unknown.</p>
Device Criticality	<p>Measure of the relative risk to the site process if the device fails:</p> <ul style="list-style-type: none"> ◦ 1 - Most critical ◦ 4 - Not critical
Purdue Level	Assigned Purdue level. The level ranges are 0–5.

Field	Description
	<p>i Note: To learn more about the Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.</p>
Zone	Area within the site location that the device is assigned to.
Site	Top-level parent entity, or industrial site, where the device is located or assigned to.

6. In the **Run** field, select a scheduled time for this job to run.

7. Select the check box next to the **Active** field.

8. Select **Submit**.

Operational Technology Manager reference

Reference topics provide additional information about the Operational Technology Manager application.

Related information

For more information about the Operational Technology (OT) product view related to the Common Service Data Model (CSDM), the Network Intrusion Detection System (NIDS), OT extension classes, and related applications see the following.

Overview

The product view and the extension classes help you understand how Operational Technology Management works with the CSDM framework and the Configuration Management Database (CMDB) respectively.

[Operational Technology product view](#)

The Operational Technology product view helps you understand how Operational Technology key entities work with the CSDM framework.

[Network Intrusion Detection System \(NIDS\) CI extension class](#)

The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.

[Operational Technology \(OT\) extension classes](#)

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

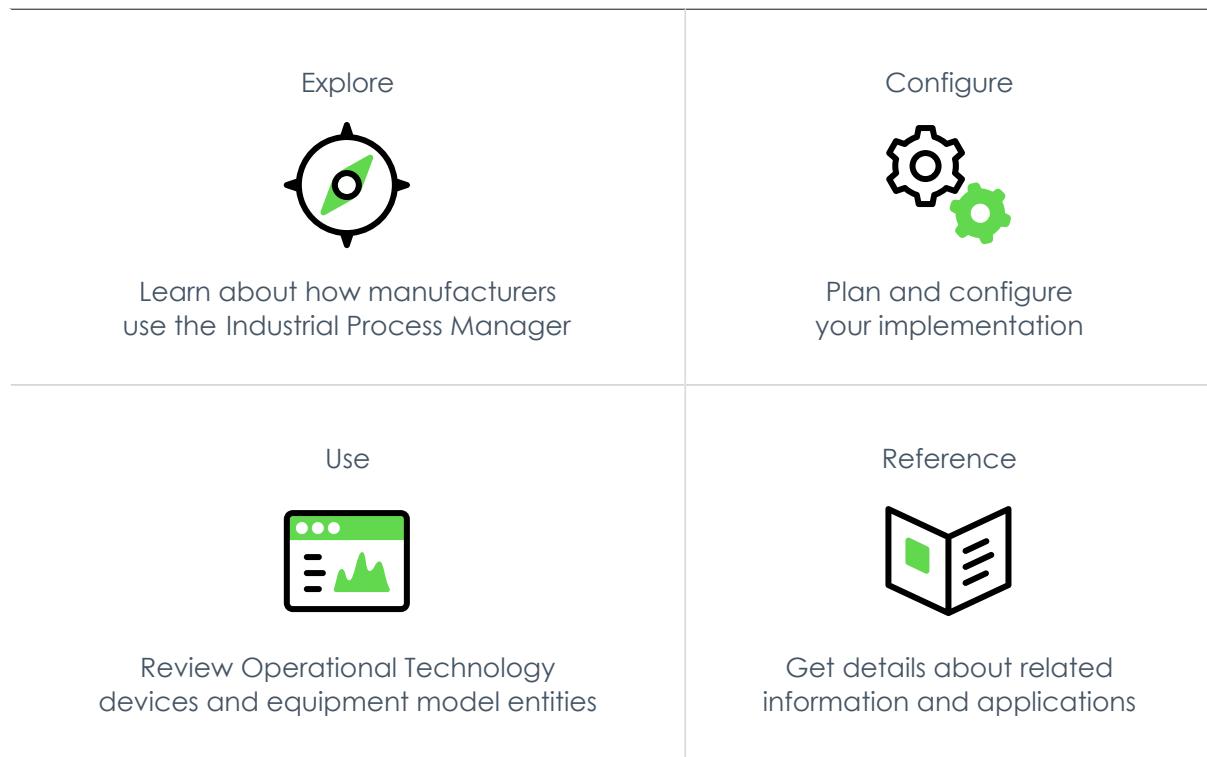
[CMDB CI Class Models store app](#)

The CMDB CI Class Models store app adds class models that extend the CMDB class hierarchy, including class descriptions, identification rules, identifier entries, and dependent relationships.

Industrial Process Manager

Use the Industrial Process Manager application to create the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Operational Technology solution. The Industrial Process Manager enables you to create your own version of the equipment models in each of your sites.

Note: The Manufacturing Process Manager was renamed to the Industrial Process Manager for Vancouver. If you're on version 1.0.9 and prior, the application is still called Manufacturing Process Manager. If you're on version 2.0, the application is called Industrial Process Manager.



Exploring Industrial Process Manager

Learn more about the common terminology, acronyms, and ISA-95 Equipment Model industry standard used in the Industrial Process Manager.

Industrial Process Manager common terminology

Before getting started with the Industrial Process Manager, let's look at some common terminology and acronyms that are used in this content.

Common terminology and acronyms

Term	Acronym	Definition
Operational Technology	OT	Technology that is used for industrial automation to control physical processes.

Common terminology and acronyms (continued)

Term	Acronym	Definition
		i Note: Operational Technology is not the Internet of Things (IoT).
International Society of Automation	ISA	Organization that publishes the standards for industrial enterprises, including the ISA-95 equipment model.
Extract, Transform, Load	ETL	Common term that is used for taking data from a source system, transforming it, and then uploading it to a target system.

ISA-95 equipment model

The ISA-95 Equipment Model is an industry standard that represents an industrial facility and the production equipment in it. You can describe the Equipment Model entities in your facilities by defining an equipment model template with different levels and level types.

With this template, you can do the following actions:

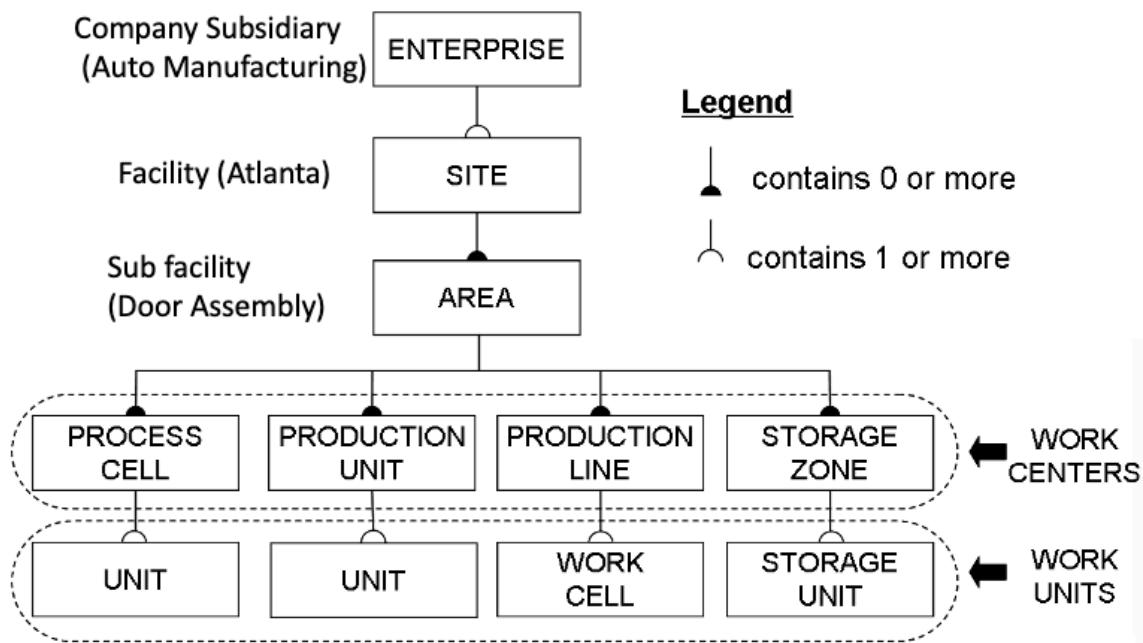
- Map your equipment model entities. With this map, you create a hierarchical structure.
- Create multiple equipment models for multiple industrial sites.
- Assign users to each site so that you can manage their access to the equipment model information for specific sites. For example, you can designate that users in Atlanta can access only the Atlanta site information but not the data for a site in Michigan. To learn more, see [Assign or remove equipment model site access for non-administrators](#)

The equipment models start at the site level and contain a detailed hierarchical structure that describes each industrial site. You apply an equipment model template to structure this data in a hierarchical sequence.

The following graphic is an example of the standard ISA-95 default template that is delivered to you when you install the Industrial Process Manager. This graphic is a representation of a facility in Atlanta that manufactures cars.

- The subordinate levels below a site represent the door assembly area, its own subordinate work centers, and work units.
- The Work Centers and Work Unit levels each have level types. In this model, there are four different level types for the Work Center level:
 - Process Cell
 - Production Unit
 - Production Line
 - Storage Zone

Equipment model template example



Equipment model templates

You can create equipment model templates you use to characterize an equipment model, or to structure the data that describes your physical industrial facility by grouping similar types of equipment model entities.

An equipment model template consists of the following components:

Equipment model template

Name and description of the equipment model template.

Equipment model template hierarchical levels

Assigned hierarchical levels that are used to sort and structure the equipment model data.

Equipment model template hierarchical level types

Types that represent different types of the areas, functions, or production processes within a hierarchical level.

To learn more about equipment templates and see a graphic example of their structure, see [ISA-95 equipment model](#) and [Defining equipment model templates](#).

Configuring the Industrial Process Manager

Configure the Industrial Process Manager application so that you can create the Equipment Model data foundation that is required for the ServiceNow® Operational Technology solution.

Note:

If you have the admin role, you can use the Industrial Guided Setup to lead you through the setup of the Industrial Process Manager application.

To access the Guided Setup, navigate to **Industrial Workspace Admin > Guided Setup**.

Task	Purpose
1. Install the Industrial Process Manager from the ServiceNow Store.	Installs the Industrial Process Manager application and supporting plugins.
2. Assign Industrial Process Manager roles.	Assigns roles to control the actions that are available for each user.
3. Populate a Microsoft Excel spreadsheet for Service Graph Connector import.	Creates and populates a Microsoft Excel spreadsheet with your existing ISA-95 Equipment Model data for upload to the Now Platform.
4. Import your Excel spreadsheet.	Uploads your existing ISA-95 Equipment Model data to the Configuration Management Database (CMDB).
5. Install Service Graph[service-graph] connectors that are provided by ServiceNow® partners, and import the equipment model data using the integrations.	Installs ServiceNow connectors that are provided by partners as they become available in the ServiceNow® Store, and imports equipment model data.
6. Grant equipment model site access to users with non-administrative roles.	Assigns or removes site access for users with assigned cmdb_ot_isa_viewer or cmdb_ot_isa_editor roles.
Optional: Automate mapping of OT devices	<p>Automates mapping of OT devices to the production process.</p> <p>Note: Enabling the mapping feature requires the following plugins:</p> <ul style="list-style-type: none"> • Operational Technology Manager • Industrial Process Manager

Install the Industrial Process Manager

If you have the required entitlement and the admin role, you can install the Industrial Process Manager application and the related plugins.

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

About this task

The following items are installed with the Industrial Process Manager:

- Plugins
- Application menu, including Guided Setup
- Roles
- Tables

For more information on viewing the components that are installed with the Industrial Process Manager application, see [Components installed with Industrial Process Manager](#).

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Industrial Process Manager application by 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 might 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.

Dependent plugins and applications appear if they will be installed, are currently installed, or must be installed. If any plugins or applications require installation, you must install them before you can install the Industrial Process Manager.

4. Optional: If demo data is available and you want to install it, select the **Load demo data** check box.
Demo data comprises the sample records that describe application features for the common use cases. Load the 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**.

Components installed with Industrial Process Manager

Several types of components may be installed with activation of the Industrial Process Manager application, including user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see [Find components installed with an application](#).

Roles installed

Role	Description
Equipment Model Viewer [cmdb_ot_isa_viewer]	Can only view the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] table records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models .
Equipment Model Editor [cmdb_ot_isa_editor]	Can view and edit the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] records.

Role	Description
	To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models .
Equipment Model Admin [cmdb_ot_isa_admin]	<p>Inherit the cmdb_ot_isa_editor role and can also do the following actions:</p> <ul style="list-style-type: none"> • Use the Industrial Guided Setup to set up the Industrial Process Manager and the Operational Technology Manager. • Edit the Equipment Model Template [isa_entity_template], [isa_entity_level], and Equipment Entity type [isa_entity_type] table records. <p>To learn more, see Industrial Workspace Admin application menu and Guided Setup.</p>
Equipment Model Downtime Planner [sn_isa_schedule_admin]	Can create, modify, and delete equipment entity schedules. Can also associate schedules with equipment entities.
Equipment Model Viewer All [cmdb_ot_isa_viewer_all]	<p>Can view all ISA Equipment Model records (cmdb_ci_ot_isa_entity) and associated Equipment Model Template records (isa_entity_template, isa_entity_level, isa_entity_type).</p> <p>Role included with cmdb_ot_admin.</p>
Amazing Admin [sn_ot_amazing_admin]	Can create, modify and delete OT subnet records (ot_subnet_mapping) for all the equipment model entity OT subnet system properties.
Amazing Editor [sn_ot_amazing_write]	Can create, modify and delete OT subnet records (ot_subnet_mapping) for all the equipment model entities associated with the user.
Amazing Viewer [sn_ot_amazing_read]	Can view OT subnet records (ot_subnet_mapping) for all the equipment model entities.

Industrial Workspace Admin application menu and Guided Setup

After you install the application and related plugins, you can use the Industrial Workspace Admin application menu to access the related Operational Technology Manager, Industrial Process Manager, Operational Technology Incident Management, Operational Technology Vulnerability Response, Operational Technology Change Management, and Operational Technology Knowledge Management functions.

Industrial Workspace Admin application menu contents

To access the Industrial Workspace Admin application menu, enter **Industrial Workspace Admin** in the application navigator. The Operational Technology Management solution currently consists of five applications:

- Operational Technology Manager
- Industrial Process Manager
- Operational Technology Vulnerability Response
- Operational Technology Incident Management, which includes Operational Technology Knowledge Management
- Operational Technology Change Management

i Note: You need to install either the Operational Technology Manager or Industrial Process Manager applications first before using Operational Technology Incident Management and Operational Technology Change Management.

The options that appear on the Industrial Workspace Admin application menu depend on which OT applications are installed and what assigned roles the user has. When the Industrial Process Manager is installed, the following functions are available on the Industrial Workspace Admin application menu:

- Guided Setup
- All OT Properties
- OT Manager, which includes the following selections:
 - OT Manager Admin
 - Industrial Process Manager
 - OT Incident Admin
 - Operational Technology Change Management

To learn more about application installation and assigned roles, see [Install the Industrial Process Manager](#) and [Assign Industrial Process Manager user roles](#).

Industrial Workspace Admin Guided Setup

If you have the admin role, you can use the Guided Setup to lead you through the setup of the Industrial Process Manager application.

To access the Guided Setup, navigate to **Industrial Workspace Admin > Guided Setup**.

The specific steps that appear as unlocked in the Guided Setup depend on which applications you have installed in your instance.

If only the Industrial Process Manager is installed, the following setup functions are locked:

- The Operational Technology Manager setup steps.
- Any Industrial Process Manager steps that depend on the Operational Technology Manager.
- The Operational Technology Vulnerability Response setup steps.
- The Operational Technology Incident Management setup steps.
- The Operational Technology Change Management setup steps.
- The Operational Technology Knowledge Management setup steps.

To learn more about Guided Setups and their use, see [Using guided setup](#).

Assign Industrial Process Manager user roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Industrial Process Manager application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the Industrial Process Manager application.

Role	Description
Equipment Model Viewer [cmdb_ot_isa_viewer]	Can only view the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] table records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models .
Equipment Model Editor [cmdb_ot_isa_editor]	Can view and edit the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models .
Equipment Model Admin [cmdb_ot_isa_admin]	Inherit the cmdb_ot_isa_editor role and can also do the following actions: <ul style="list-style-type: none"> • Use the Industrial Guided Setup to set up the Industrial Process Manager and the Operational Technology Manager. • Edit the Equipment Model Template [isa_entity_template], [isa_entity_level], and Equipment Entity type [isa_entity_type] table records. To learn more, see Industrial Workspace Admin application menu and Guided Setup .
Equipment Model Downtime Planner [sn_isa_schedule_admin]	Can create, modify, and delete equipment entity schedules. Can also associate schedules with equipment entities.
Equipment Model Viewer All [cmdb_ot_isa_viewer_all]	Can view all ISA Equipment Model records (cmdb_ci_ot_isa_entity) and associated Equipment Model Template records (isa_entity_template, isa_entity_level, isa_entity_type). Role included with cmdb_ot_admin.

Role	Description
Amazing Admin [sn_ot_amazing_admin]	Can create, modify and delete OT subnet records (ot_subnet_mapping) for all the equipment model entity OT subnet system properties.
Amazing Editor [sn_ot_amazing_write]	Can create, modify and delete OT subnet records (ot_subnet_mapping) for all the equipment model entities associated with the user.
Amazing Viewer [sn_ot_amazing_read]	Can view OT subnet records (ot_subnet_mapping) for all the equipment model entities.

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

View and edit OT system properties

View and edit all of the Operational Technology (OT) related system properties for different applications.

Before you begin

Role required: admin

About this task

You can modify the system properties for the following OT applications from **All OT Properties** module on the Now Platform.

- Discovery for Operational Technology
- Industrial Process Manager
- ISA Equipment Model
- Operational Technology Manager
- Operational Technology Incident Management
- Operational Technology Knowledge Management
- Operational Technology Change Management

Procedure

1. Navigate to **All > Industrial Workspace Admin > All OT Properties**.
2. In the System Properties table, select the application that you want to edit the system properties for.
3. Edit the available system properties as needed for the application.
4. Select **Update**.

Defining equipment model templates

Create templates that you can assign to the equipment model entities that you created in the Now Platform. You can use these templates to characterize an equipment model or structure the data that describes your physical industrial facility by grouping similar types of equipment model entities.

Create an equipment model template

Create an equipment model template record that identifies and describes the use of the template. After you create an equipment model template, you can create hierarchical levels and types for it.

Before you begin

Role required: cmdb_ot_isa_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Template**.
2. Click **New**.
3. On the form, fill in the fields.

Equipment model template form

Field	Description
Name	Name of the equipment model template.
Description	Description of the equipment model template.
Application	Selected application scope. Global appears if this scope is the global application scope.

4. Click **Submit**.

What to do next

Create hierarchical sorting levels for the equipment model template.

Create hierarchical sorting levels for an equipment model template

Create and assign hierarchical levels for your equipment model template. When you assign an equipment template to an equipment model, these levels sort and structure the data you see in it.

Before you begin

Role required: admin

About this task

You can assign levels to an equipment model template for sorting purposes. For example, you can assign Site, Area, Work Center and other levels to the equipment, and designate the sorting sequence for each.

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Template**.
2. Select an equipment model template.
3. In the Template Levels related list, click **New**.
4. On the form, fill in the fields.

Template Level form

Field	Description
Level name	<p>Name of the level to which you are assigning the equipment model. Examples include:</p> <ul style="list-style-type: none"> Site An industrial site. Area An area in an industrial site. Work Center A work center in an industrial site.
Parent	<p>Identifier for the equipment model template level above this level. If left empty, this level is the top level in the model. For example, you can do the following actions:</p> <ul style="list-style-type: none"> ◦ If you are creating a Site level, leave this field empty if it is the top level of the equipment model hierarchy that does not have a parent. ◦ If you are creating an Area level, and it is a child to the Site level, select Site as its parent. ◦ If you are creating a Work Center level, and it is a child to the Area level, select Area as its parent.
Application	Selected application scope. Global appears if this scope is the global application scope.
Template	Name of the selected equipment model template.
Order	Number that indicates the position of the level in the equipment model hierarchy for sorting purposes. The smallest number entered represents the highest hierarchical level. For example, enter 1 for Site if the site

Field	Description
	represents the highest level in the hierarchy for the equipment model template.

5. Click **Submit.**

What to do next

Create granular types within an equipment model template hierarchical level.

Create equipment model level types

Create granular level types within each equipment model template level that you created. The granular level types that you create within that level describe the type of production processes within it.

Before you begin

Role required: admin

About this task

You can create types that represent the different types of locations, areas, or functions within a level. For example, in the ISA 95 template, the Work Center level has the following level types:

- Production Cell
- Production Unit
- Production Zone
- Storage Zone

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Template**.
2. Select an equipment model template.
3. In the Template Levels related list, select an equipment model template level.
4. In the Template Types related list, click **New**.
5. On the form, fill in the fields.

Template Level Type form

Field	Description
Level type name	Name of the level type that you are assigning to the selected equipment model template level. For example, you assign Production Cell to create a Production Cell type for a Work Center level.
Level name	Name of the selected equipment model template level.
Application	Selected application scope. Global appears if this scope is the global application scope.

Field	Description
Template	Name of the selected equipment model template.

6. Click **Submit**.

Importing equipment model data

The scheduled import function enables you to import your existing equipment model data from a populated Microsoft Excel flat-file spreadsheet. You can use it to import your ISA-95 Equipment Model data to the Configuration Management Database (CMDB).

You must install the Industrial Process Manager before importing equipment model data.

Several methods are available for importing the equipment model data into the Now Platform:

- If you use the spreadsheet to import the data, you must populate the Microsoft Excel spreadsheet with your existing ISA-95 Equipment Model data and run the **SG-Equipment Model Scheduled Import Using Spreadsheet** scheduled import. Many legacy record systems contain functions that enable you to export this data to an Excel spreadsheet, which means that you don't have to populate it manually.
- Several ServiceNow partners are also developing integrations to third-party legacy record systems that store equipment model data.
 - When these integrations become available, you can find them on the ServiceNow Store by searching for Operational Technology certified integrations for the Industrial Process Manager.
 - Install those integrations that are applicable to your environment, and run them as needed.

By using these import methods, you can update existing equipment models in the Now Platform with the data that is stored in your authoritative source when needed. For newly imported data, the Now Platform automatically creates Equipment Model Entity CI class records in the Configuration Management Database (CMDB).

System properties that affect import processing

The following system properties affect how you populate your Microsoft Excel spreadsheet with the equipment model data and how the Import Equipment Model - ETL process functions.

`sn_isa_model.cmdb_relationships_sync_levels`

Determines how many levels of an equipment model can be imported into the Now Platform and then are synchronized in the Configuration Management Database (CMDB). The default value is 8.

`sn_isa_model.short_code_validation_max_length`

Sets the maximum length for the Short Code column on your spreadsheet. The default value is 3.

`sn_isa_model.user_search_matching_attribute`

Matches the user data references that are imported from your populated spreadsheet to the corresponding user records that are stored in the System Users [sys_user] table. The default is the user's email address, because the email address is unique to each user record.

`glide.scriptable.excel.max_file_size`

Sets the maximum size of an Excel file, expressed in bytes. This property is global.

Note: To learn more about adding or creating system properties to control system behavior, see [Add a system property](#).

Populating your Microsoft Excel spreadsheet with equipment model data

Create and populate a Microsoft Excel spreadsheet with your existing ISA equipment model data. Positioning your existing data in the correct columns is crucial to the success of your upload.

To create a Microsoft Excel spreadsheet that properly populates the Configuration Management Database (CMDB) in the Now Platform, do the following actions:

1. Prepare your spreadsheet for upload by using the Microsoft Excel spreadsheet that is attached to the data source record. To locate an empty template, do the following actions:
 - a. Navigate to **Equipment Model - ISA > Import Equip. Model - Data Source**
 - b. Click **Import Equipment Model – Data Source - v2.xlsx**

Note: Alternately, to download the **Import Equipment Model – Data Source - v2.xlsx** spreadsheet, see the [Microsoft Excel spreadsheets required for the ISA Equipment Model Excel Service Graph Connector \[KB0966600\]](#) article in the Now Support Knowledge Base.

2. Download the attached Import Equipment Model – Data Source - v2.xlsx spreadsheet to learn more about the template and its worksheets:

Note: If you're an ISA SGC user upgrading from v1 to v2, see the section named [Upgrading from v1 to v2](#) below.

Import Equipment Model – Data Source - v2.xlsx spreadsheet

Worksheet name	Purpose
Blank template for data import	Populates your Equipment Model data for import. You can view detailed examples in the remainder of this topic.
Data Column Descriptions	Provides descriptions of the data columns on the spreadsheet, similar to the information found in this topic.
Sample Data for Import	Provides an example of an equipment model for import in the spreadsheet. You can view these examples in the remainder of this topic.

3. After populating the Microsoft Excel spreadsheet, save it in a known location for easy access when you run the Integration Hub ETL function.

Note: Column names cannot be changed. You can add additional columns to support additional fields to uniquely identify owners, as designated in the `sn_isamodel.user_search_matching_attribute` system property.

Populating the spreadsheet

Sample Operational Technology data, columns A through J

You can import data from multiple sites in a single spreadsheet. The example image shows data for two sites: ATL and CTL.

	A	B	C	D	E	F	G	H	I	J
1	Path	Short Code	Entity Name	Location	Assigned to	Support Group	Description	Process criticality	Company	Template
2	ATL	ATL	Atlanta Site	Atlanta Car Facility	fred.juddy@example.com	Atlanta Plant Support	the site in Atlanta where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
3	ATL-B64	B64	Building 64	Atlanta Building 64	fred.juddy@example.com	Atlanta Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template
4	ATL-B42	B42	Building 42	Atlanta Building 42	fred.juddy@example.com	Atlanta Plant Support	similar to Building 64 except with a 42 on the side	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
5	ATL-B64-MASS	MASS	Model M	Atlanta Building MASS	fred.juddy@example.com	Atlanta Plant Support	model S needs to be assembled somewhere	1 - most critical	Demo Car Corp	ISA 95 Default Template
6	ATL-B64-QASS	QASS	Model Q	Atlanta Building QASS	fred.juddy@example.com	Atlanta Plant Support	a place for the Q model to get assembled	1 - most critical	Demo Car Corp	ISA 95 Default Template
7	ATL-B64-MPROD	MPROD	Model MPROD	Atlanta Building MPROD	fred.juddy@example.com	Atlanta Plant Support	Model S also needs a production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
8	ATL-B64-QPROD	QPROD	Model QPROD	Atlanta Building QPROD	fred.juddy@example.com	Atlanta Plant Support	Model Q production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
9	ATL-B42-MQSTOR	MQSTOR	Model M and Q	Atlanta Building MQSTOR	fred.juddy@example.com	Atlanta Plant Support	storage for the models we built	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
10	ATL-B64-QPROD-C1	C1	Cell 1	Atlanta Building C1	fred.juddy@example.com	Atlanta Plant Support	Q prod assembly cell 1	1 - most critical	Demo Car Corp	ISA 95 Default Template
11	ATL-B64-QPROD-C2	C2	Cell 2	Atlanta Building C2	fred.juddy@example.com	Atlanta Plant Support	Q prod assembly cell 2	1 - most critical	Demo Car Corp	ISA 95 Default Template
12	ATL-B42-MQSTOR-Z1	Z1	Zone 1	Atlanta Building Z1	fred.juddy@example.com	Atlanta Plant Support	storage zone for MQ for transfer	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
13	ATL-B42-MQSTOR-Z6	Z6	Zone 2	Atlanta Building Z6	fred.juddy@example.com	Atlanta Plant Support	storage zone for MQ to just store the stuff	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
14	CTL	CTL	California Site	California Car Facility	fred.juddy@example.com	California Plant Support	the site in California where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
15	CTL-C64	C64	Building 64	California Building 64	fred.juddy@example.com	California Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template

Columns A through J

Column	Name	Type	Description	Required
A	Path	string	<p>Concatenation of the short codes of this entity and all its parent entities. For example, ATL-B42-MQSTOR-Z1 is the concatenation of these short codes:</p> <ul style="list-style-type: none"> • ATL short code for the Atlanta site. • B42 short code for Building B42. • MQSTORE short code for Model M and Q. • Z1 short code for the Zone 1 transfer storage zone for Model M and Q. 	Yes
B	Short Code	string, alphanumeric only	<p>Short description code for the entity. Refer to the previous Path column description for examples of short codes.</p> <p>The Short Code can be no longer than the maximum length that is designated in the <code>sn_is_a_model.short_code_validation_max_length</code> system property.</p>	No
C	Entity Name	string	Long name of the entity. For example, a city name, a building number, or a model number.	Yes
D	Location	string	Location of the entity. For example, you would list Atlanta Building 64 for each of the equipment models that are located there. The cmn-location value that is stored in the Configuration Management Database (CMDB) in the Now Platform, which uses it as a reference.	No

Columns A through J (continued)

Column	Name	Type	Description	Required
E	Assigned to	string	Email address of the assigned person who owns and manages this entity record. i Note: You can use additional attributes, based on the settings designated in the <code>sn_isamodel.user_search_matching_attribute</code> system property.	No
F	Support Group	string	Name of the group that supports the maintenance and management of this entity.	No
G	Description	string	Long description of this equipment model entity and its purpose.	No
H	Process criticality	string	Measure of how critical, or important, the entity is to the industrial process. Examples are as follows: <ul style="list-style-type: none">• 1 - most critical.• 2 - somewhat critical.	No
I	Company	string	Name of the company that the entity belongs to. The cmn-location value that is stored in the CMDB in the Now Platform, which uses it as a reference.	No
J	Template	string	The template used to import data. i Note: After your import your data, you cannot set the template.	Yes

Upgrading from v1 to v2

If you're an ISA SGC user upgrading from v1 to v2, you can import new ISA equipment model entities that have a unique path and update existing ISA equipment model entities that already have a path value with a fix script.

Import your equipment model data using the data source and scheduled import

After you complete your Microsoft Excel spreadsheet with your equipment model data, import it into the Now Platform by using the data source and scheduled import.

Before you begin

Before you perform this process, you must prepare a Microsoft Excel spreadsheet for import. To learn more, see [Populating your Microsoft Excel spreadsheet with equipment model data](#).

Role required: cmdb_inst_admin, import_admin

About this task

By running this process, you create unique Equipment Model Entity CI class records in the Configuration Management Database (CMDB) for the equipment model records that are included in your spreadsheet.

Procedure

1. Navigate to **All > Equipment Model - ISA > Import Equip. Model - Data Source**.
2. In the **SG Equipment Model** data source record, attach the Microsoft Excel spreadsheet that you created:
 - a. Select **Manage Attachments**.
 - b. In the Attachments dialog box, select **Choose File**.
 - c. Select the Microsoft Excel spreadsheet that you created, and then close the Attachments dialog box.
 - d. After attaching the spreadsheet, select the **Load All Records** related link to load all records from the spreadsheet to the import table. Once the operation is complete, you should see the following confirmation message with the **Success** completion code if the data is loaded without any

Progress	
Name	ImportProcessor
State	Complete
Completion code	Success
Message	Processed: 25, inserts 0, updates 0, errors 0, empty and ignored 25, ignored errors 0 (0:00:00.087)

Next steps...

- [Import sets](#) Go to the import sets for this data load
- [Loaded data](#) Go to the newly imported data inside the staging table: sg_isa_entity_import
- [Run Robust Transform](#) Transform a loaded import set using a robust transform
- [Import log](#) View the import log
errors.

- e. In the confirmation message, select the **Run Robust Transform** related link.
- f. Select **Transform**. If the import is successful, you should see the following confirmation message with the **Success** completion

Progress

Name	Transforming: ISET0010001
State	Complete
Completion code	Success
Message	Transformation complete

Next steps...

- [ISET0010001](#) Go to the import sets for this data load
- [Transform history](#) Show the transform history, related errors and log
- [Import log](#) View the import log
code.

Assign or remove equipment model site access for non-administrators

Assign or remove equipment model site access for non-administrators by creating user criteria to determine whether certain users can access equipment model entities for specific sites.

Before you begin

Role required: admin

About this task

Use user criteria to determine whether certain users can read or edit equipment model entities for specific sites. After you create a user criteria record, you can assign it to a site to control who can read and edit the equipment model entities. You can further assign OT roles to users or groups to allow access to OT devices assigned to those same sites. For more information, see [Assign Operational Technology Manager roles](#).

- Note:** Users upgrading to version 1.0.12 have their site user access migrated to user criteria and groups. For more information, see [Migrating site user access to user criteria and groups](#).

Procedure

1. Navigate to **All > Knowledge Management > Administration > User Criteria**
2. Select **New**.
3. On the form, fill in the fields.

User criteria form fields

Field	Description
Name	Name of the user criteria.
Short description	Brief description of the user criteria to access the site's equipment model entities.
Users	Users who can access the site's equipment model entities when you apply the user criteria. Click the unlock users icon () to select users. Click the add me icon () to add yourself as a user.
Groups	Groups who can access the site's equipment model entities when you apply the user criteria. Click the unlock groups icon () to select the groups.
Roles	Roles who can access the site's equipment model entities when you apply the user criteria. Click the unlock roles icon () to select the groups.
Advanced	Option to create a script for the user criteria.
Application	This field is automatically set to Global.
Active	Option to make the user criteria available.

Field	Description
Companies	Companies who can access the site's equipment model entities when you apply the user criteria. Click the unlock companies icon () to select the companies.
Locations	Locations which can access site's equipment model entities when you apply the user criteria. Click the unlock locations icon () to select the locations.
Departments	Departments who can access site's equipment model entities when you apply the user criteria. Click the unlock departments icon () to select the departments.
Match All	Option to make every condition required when the user criteria is applied. The conditions are set in the previous fields, such as Location , Department , and so on

What to do next

After you create the user criteria, you can assign it to a site. For more information about assigning Can Edit access to a site, see [Assign user criteria for Can Edit access to a site](#). For more information about adding Can Read access to a site, see [Assign user criteria for Can Read access to a site](#).

Assign user criteria for Can Read access to a site

Assign user criteria to a site define which users can read or view the equipment model entities that belong to the selected site.

Before you begin

Role required: cmdb_ot_isa_admin or admin

About this task

You can assign user criteria for Can Read access in two locations:

- From the Equipment Model Entity View Access table
- From the Can Read Equipment Models related list in a site record

Procedure

1. Navigate to one of the following locations:

- **All > Equipment Model - ISA > User Criteria - Can Read** for the Equipment Model Entity View Access Table
- **All > Equipment Model - ISA > Sites** and open a site record. Select the Can Edit Equipment Models related list.

2. Select **New** to create a new record.

3. In the **Site** field, select the appropriate equipment model site record.

4. In the **User Criteria** field, select the appropriate user criteria that defines which users can read or view the selected site's equipment model entities.

Note: The same users can also view the OT devices assigned to the selected site if they're assigned the cmdb_ot_viewer role.

They can edit the OT devices assigned to the selected site if they're assigned a cmdb_ot_editor role.

5. Click **Submit**.

Assign user criteria for Can Edit access to a site

Assign user criteria to a site define which users can edit the equipment model entities that belong to the selected site.

Before you begin

Role required: cmdb_ot_isa_admin or admin

About this task

You can assign user criteria for Can Edit access in two locations:

- From the Equipment Model Entity Edit Access table
- From the Can Edit Equipment Models related list in a site record

Procedure

1. Navigate to one of the following locations:

- All > **Equipment Model - ISA > User Criteria - Can Edit** for the Equipment Model Entity Edit Access Table
- All > **Equipment Model - ISA > Sites** and open a site record. Select the Can Edit Equipment Models related list.

2. Select **New** to create a new record.

3. In the **Site** field, select the appropriate equipment model site record.

4. In the **User Criteria** field, select the appropriate user criteria that defines which users can edit the selected site's equipment model entities.

Note: The same users can also view the OT devices assigned to the selected site if they're assigned the cmdb_ot_viewer role.

They can edit the OT devices assigned to the selected site if they're assigned a cmdb_ot_editor role.

5. Click **Submit**.

Managing an equipment model entity schedule

You can manage an equipment model entity schedule with the Industrial Process Manager application. By using a schedule, you can track several maintenance tasks for one equipment model entity.

Overview

You can link schedules to any equipment model entity. If you have the Equipment Model Downtime Planner role (sn_isa_schedule_admin), you can add, modify, or delete the schedule entries of an equipment model entity and do the following tasks:

- Maintain the schedules for the various equipment model entities.
- Associate these schedules with equipment model entities.
- Pick a time slot from a schedule so that you can work on an Operational Technology (OT) incident or remediation task. For more information, see [Select a start time for an OT remediation task](#).

Examples

Let's say that you want to set multiple schedule entries for one equipment model entity schedule. These entries complete different tasks and occur at different times. You can do so by creating schedule entries in the Schedule Entries related link of the existing equipment model entity schedule record.

If you no longer want a schedule associated with an equipment model entity, you can detach the schedule by using the Schedules related link in the equipment model entity record.

If you want to view existing schedules for an equipment model entity, you can do so in the Equipment Model Workspace or in the Planned Downtime module on the Platform.

Create an equipment model entity schedule

Create an equipment model entity schedule with the Industrial Process Manager application. With these schedules, you can easily maintain multiple equipment model entities.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Entity Schedules**.
2. Select **New**.
3. On the form, fill in the fields.

Equipment model entity schedules form

Field	Description
Name	Unique name for the schedule.
Time zone	<p>Time zone for the schedule. If you select Floating, the time zone is relative to whatever process is accessing the item at.</p> <p>For example, if a resource manager in Amsterdam sets a floating schedule for 8:00 to 17:00, a user in San Jose, California, also sees the schedule as 8:00 to 17:00. When you define a schedule in one time zone, users in different time zones see the schedule in their own time zone.</p>
Type	Text label that describes the purpose of the schedule.

Field	Description
Description	Description of the schedule.

4. Select **Submit**.

What to do next

Now, you can create the entries for an equipment model entity schedule. For more information, see [Create a schedule entry](#).

Create a schedule entry

Create a schedule entry for an existing equipment model entity schedule in the Industrial Process Manager application. You can create more than one entry for a schedule. Schedule entries allow multiple maintenance tasks to take place for one equipment model entity.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Entity Schedules**.
2. Select an existing equipment model entity schedule record.
3. Select the **Schedule Entries** related link.
4. Select **New**.
5. On the form, fill in the fields.

Schedule entries form

Field	Description
Name	Unique name for the schedule entry.
Type	Label that describes the purpose of the schedule.
Show as	Option that indicates how the schedule entry should appear in calendar applications.
Repeats	Repetition interval for the schedule entry, if any. If you select a repetition interval, other fields appear so that you can further specify the repeat interval.
Repeat every	Scheduling repetition frequency - weekly, monthly, or yearly. This field appears only when Daily , Weekly , Monthly , or Yearly is selected from the Repeats field.
Repeat on	Days of the week that a weekly schedule repeats on. This field appears only when Weekly is selected from the Repeats field.
Monthly type	Monthly schedule repetition frequency. This field appears only when Monthly is selected from the Repeats field. Options include:

Field	Description
	<ul style="list-style-type: none"> ◦ Repeat on a specific day of the month. ◦ Repeat on a specific day in a specific week of the month. ◦ Repeat on the last day of the month. ◦ Repeat on a specific weekday in the last week of the month.
Yearly type	<p>Yearly schedule repetition frequency. This field appears only when Yearly is selected from the Repeats field. Options include:</p> <ul style="list-style-type: none"> ◦ Repeat on a specific day of the year. ◦ Repeat on a floating day.
Float week	Week of the month that a floating yearly schedule repeats on. This field appears only when Floating is selected from the Yearly field.
Float day	Day of the week that a floating yearly schedule repeats on. This field appears only when Floating is selected from the Yearly field.
Month	Month of the year that a floating yearly schedule repeats on. This field appears only when Floating is selected from the Yearly field.
Repeat until	Repetition end date. If you leave this field empty, the schedule repeats indefinitely.

6. Select **Submit**.

Result

Your schedule entry is created, and now you can edit and update the entry as necessary.

Associate a schedule with an equipment model entity

Create one or more maintenance schedules for an equipment model entity, edit an existing schedule, or delete schedules with the Industrial Process Manager application.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Planned Downtime**.
2. Select the equipment model entity that you want to associate with a schedule.
3. Select the **Schedules** related link.
4. Optional: To add a new schedule for the selected equipment model entity, do these actions:

- Select **New**.
 - Fill in the form and select **Submit**.
- 5.** Optional: To delete a schedule for the selected equipment model entity, do these actions:
- Select the schedule that you want to delete.
 - Select **Delete**.
- 6.** Optional: To edit a schedule for the selected equipment model entity, do these actions:
- Select the schedule that you want to edit.
 - Add your changes and select **Update**.

Result

The maintenance schedule is created, deleted, or edited. Depending on the steps you followed, an eligible user can see the new schedule, no longer see the deleted schedule, or see the edited version of the schedule.

Attach a schedule to an equipment model entity

Attach an existing schedule to an equipment model entity with the Industrial Process Manager application. Attaching a schedule to an equipment model entity applies the schedule and its entries to that entity.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All > Equipment Model - ISA > Equipment Model Entities**.
2. Select an equipment model entity record.
3. Select the **Schedules** related link.
4. Select **Edit**.
5. In the Collection list, select the schedule that you want to attach to the equipment model entity.
6. Move the selected schedule to the Schedules list by using the middle arrows.
7. Select **Save**.

Result

The attached schedule is now applied to the equipment model entity. You can view and manage the attached schedule in the equipment model entity record.

Detach a schedule from an equipment model entity

Detach an existing schedule from an equipment model entity with the Industrial Process Manager application. If a schedule no longer applies to an equipment model entity, you can easily remove it so that it doesn't show up for that entity.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All > Equipment Model - ISA > Equipment Model Entities**.
2. Select an equipment model entity record.

3. Select the **Schedules** related link.
4. Select **Edit**.
5. In the Schedules List, select the schedule that you want to detach from the equipment model entity.
6. Move the selected schedule to the Collection list by using the middle arrows.
7. Select **Save**.

View a schedule for the equipment model entity

View a schedule for an existing equipment model entity in the Industrial Process Manager application.

Before you begin

Role required: cmdb_ot_isa_viewer

About this task

You can view equipment model entity schedules in two places depending on where you're working:

- The Equipment Model Workspace
- The Planned Downtime module on the Platform

Procedure

1. To view the equipment model entity schedules in the Equipment Model Workspace, do these actions:
 - a. Navigate to the **Equipment Model Workspace**.
 - b. Select an equipment model entity record.
 - c. Select **View schedules**.
 - d. View the downtime slots for that equipment model entity.
2. To view the equipment model entity schedules in the Planned Downtime module, do these actions:
 - a. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Planned Downtime**.
 - b. View the association of the schedules and equipment model entities.

Add a child schedule

Add a child schedule to an existing equipment model entity schedule with the Industrial Process Manager application. When you make adjustments to the child schedule, it also applies to the parent schedule. For example, you might want to extend the scheduled time on a particular day or remove the holidays from a schedule.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Entity Schedules**.
2. Select a record for an existing equipment model entity schedule.
3. Select the **Child Schedules** related link.

4. Select **Edit**.
5. Select the desired schedule in the Collection list.
6. Move the selected schedule to the Child Schedules list by using the middle arrows.
7. Select **Save**.

Result

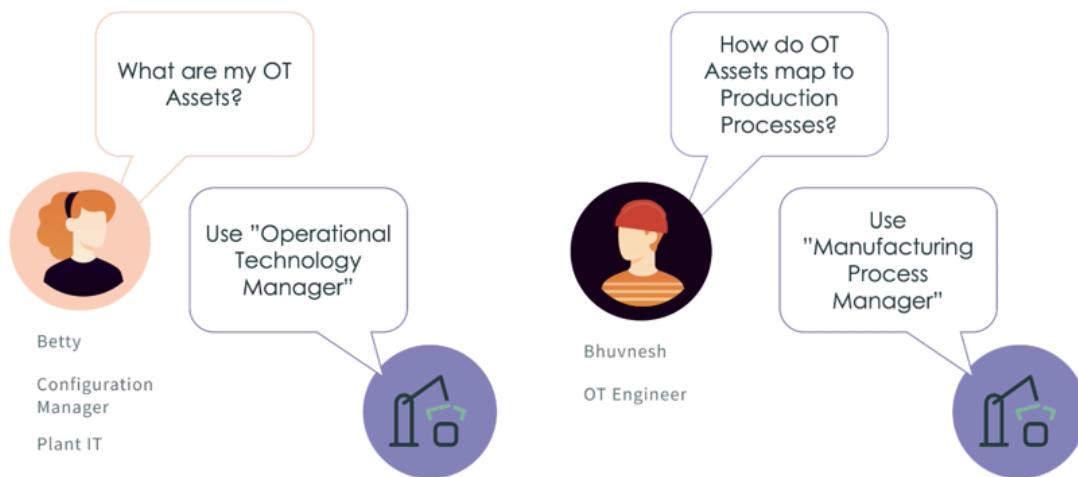
The selected child schedule now applies to the parent schedule.

Using Industrial Process Manager with the Operational Technology Manager

After you complete all required set up tasks, including importing equipment models, you can use the Operational Technology Manager and Industrial Process Manager functions on the Industrial Workspace Admin menu. These functions include the Equipment Model Workspace and the Operational Technology Manager Workspace landing page.

The following graphic shows some common questions that industrial personnel ask about operational problems in an enterprise, and the Now Platform functions you use to answer them. These functions help your personnel visualize data relationships in your industrial facilities.

Industrial personnel questions about operational problems



Betty, a Configuration Manager, works at the enterprise level and wants to know where the OT devices reside in the enterprise. To answer this question, a Configuration Manager can use the Operational Technology Manager functions on the Industrial Workspace Admin menu. To learn more, see [Operational Technology Devices landing page tab](#).

Bhuvnesh, an OT engineer, works at the site level and wants to know how OT devices map to specific production processes. For example, a question asked might be "What HMs and PLCs are controlling this specific portion of the industrial processing? To answer this question, an OT Manager at the site level can use the Industrial Process Manager functions on the Industrial Workspace Admin menu.

Managing equipment models

The Equipment Model Workspace enables you to review and manage ISA-95 equipment model data. You use it to review imported equipment model data or to manually create an equipment model.

An equipment model maps the operational elements of a particular facility. For example, an industrial facility in Atlanta that stores materials, and uses them to produce cars. Using the Equipment Model Workspace, you can view selected equipment model entities for specific industrial sites, and perform the following tasks:

- View a graphical representation of an equipment model hierarchy and its relationship to other entities.
- View or map upstream or downstream production processes.
- Review child entities.
- Review or associate additional OT devices with the selected equipment model entity

Note: Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Review and update the equipment model details

Review and update the details for an equipment model that you imported into the Now Platform so that you can make sure that the information is correct. You can also manually create a new equipment model entity and then add details to it.

Before you begin

Import equipment model data to the Now Platform. To learn more, see [Importing equipment model data](#).

Role required: cmdb_ot_isa_viewer, cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

If you have an assigned cmdb_ot_isa_viewer role, you can only view equipment model entities. If you have any of the other assigned cmdb_ot_isa roles, you can also edit equipment model entities.

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Workspace**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
You can search for a site by typing in the site name or its short code.
3. Review an existing equipment model entity, or create one.

Task	Description
Review and update an existing equipment model	In the selector pane, do the following actions: a. Expand the equipment model hierarchy. b. Click the entity that you want to view.
Create an equipment model entity and populate the details	a. Click Create new entity . b. In the Create new entity form, fill in the details. To learn more, see Create an entity for a new equipment model .

Task	Description
	<p>c. Click Save.</p> <p>d. Use the Equipment model view details form to enter the remaining details for the new equipment model entity.</p>

4. On the form, review and update the fields.

Equipment model details form

Field	Description
Entity name	Name of the equipment model entity.
Parent	<p>Name of the entity, if any, that is the parent to this equipment model entity. This field is empty for the top-level parent entity, which has no parent. The top-level parent entity is referred to as a site.</p> <p>i Note: You can update the Parent field after the equipment model entity is created.</p>
Template	<p>Equipment model template that is assigned to an equipment model entity you manually create.</p> <p>i Note: You can't assign an equipment model template to an equipment model that you imported into the Now Platform® using the Integration Hub ETL or a third-party integration.</p>
Level	<p>Hierarchical level that is assigned from the selected equipment model template for data sorting and structuring purposes. Examples are as follows:</p> <ul style="list-style-type: none"> Site Industrial site. Area Area in an industrial site. Work Center Work center in an industrial site. <p>Search for and select an equipment level to assign to the equipment model entity. To learn more, see Create hierarchical sorting levels for an equipment model template.</p>
Type	Name of the level type that is assigned to the equipment model template level. For example, Material Assembly or Production

Field	Description
	Cell for a Work Center level. To learn more, see Create equipment model level types .
Short description	Short description of this equipment model entity and its purpose.
Short Code	Short code that is assigned to this equipment model entity.
Path	<p>Concatenation of the short codes of this equipment model entity and all its parent entities. For example, ATL-B42-MQSTOR-Z1 is the concatenation of the following short codes:</p> <ul style="list-style-type: none"> ◦ ATL short code for the Atlanta site. ◦ B42 short code for Building B42. ◦ MQSTORE short code for Model M and Q. ◦ Z1 short code for the Zone 1 transfer storage zone for Model M and Q.
Location	Location of the equipment model entity. For example, Atlanta Building 64 would be the location for each associated equipment model that is located there. Search for and select the location to assign to the equipment model entity.
Company	Name of the company that is associated with the equipment model entity. Search for and select a company to assign to the entity.
Assigned to	Assigned user who operates and handles this equipment model entity. Search for and select the user to assign to the entity.
Managed by	Name of the assigned person who owns and is responsible for managing this entity record. Search for and select the user to assign to the equipment model entity.
Process criticality	<p>Measure of how critical, or important, the equipment model entity is to the industrial process. Select the process criticality for the entity. For example:</p> <ul style="list-style-type: none"> ◦ 1 - most critical. ◦ 2 - somewhat critical.
Support Group	Name of the group that supports this equipment model entity. Search for and select the user group to assign to the equipment model entity.
Managed by Group	Name of the assigned group that owns and is responsible for managing this entity

Field	Description
	record. Search for and select the user group to assign to the entity.
Company	Name of the company that the equipment model entity belongs to. The core_company value is stored in the CMDB in the Now Platform as a reference.
Operational status	Current operational status of the equipment model entity: Operational Entity that is fully operational in the production process. Non-Operational Entity that is non-operational in the production process.

5. Review the associated equipment model data in the related list tabs as follows:

Task	Description
View the equipment model hierarchy	See View the equipment model hierarchy .
Map the upstream production processes for the equipment model entity.	<p>a. Click Upstream Process.</p> <p>b. To learn more, see Map the upstream production processes for the selected equipment model entity.</p>
Map the downstream production processes for the equipment model entity.	<p>a. Click Downstream Process.</p> <p>b. To learn more, see Map the downstream production processes for the selected equipment model entity.</p>
View the child entities for the equipment model entity.	<p>a. Click Child Entities.</p> <p>b. To learn more, see Review the child entities for the equipment model entity.</p>
View the OT devices that are associated with the current equipment model entity and its child entities.	<p>a. Click Mapped OT Devices.</p> <p>b. To learn more, see Add OT devices that are associated with the selected equipment model entity.</p> <p>i Note: By default, you cannot see OT control modules in this list.</p>

6. When you finish reviewing and updating the equipment model details, do one of the following actions.

Action	Description
Save the updated equipment model entity	Click Save .
Delete the equipment model entity	Click Delete .

7. Optional: To view different OT data associated with the equipment model entity and its child entities, you can select the following related lists in the equipment model entity record:
- Mapped OT Devices
 - OT Incidents
 - OT Change Requests
 - Vulnerable Items
 - Remediation Tasks

Create an entity for a new equipment model

Create an entity for a new equipment model. You do this task when you want to manually create a new equipment model entity directly in the Now Platform rather than import the equipment model data from an external source.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
You can search for a site by typing in the site name or its short code.
3. Click **Create new entity**.
4. On the form, fill in the fields.

Create new entity form

Field	Description
Parent	<p>Name of the entity, if any, that is the parent to this entity.</p> <p>The currently selected equipment model appears as the parent entity. To change the parent, search for and select the entity that is a parent to the entity that you are creating.</p>

Field	Description
Entity name	Name of the equipment model entity.
Short Code	Short code that is assigned to this entity.
Entity type	<p>Name of the level type that is assigned to the equipment model template level. For example, Material Assembly or Production Cell for a Work Center level.</p> <p>Search for and select an entity type. To learn more, see Create equipment model level types.</p>

5. Click **Save.**

6. In the Details form, enter the remaining details for the new equipment model entity.

To learn more, see [Review and update the equipment model details](#).

View the equipment model hierarchy

View a graphical representation of the hierarchical structure of the selected equipment model entity, and its relationships to other entities in the production process.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

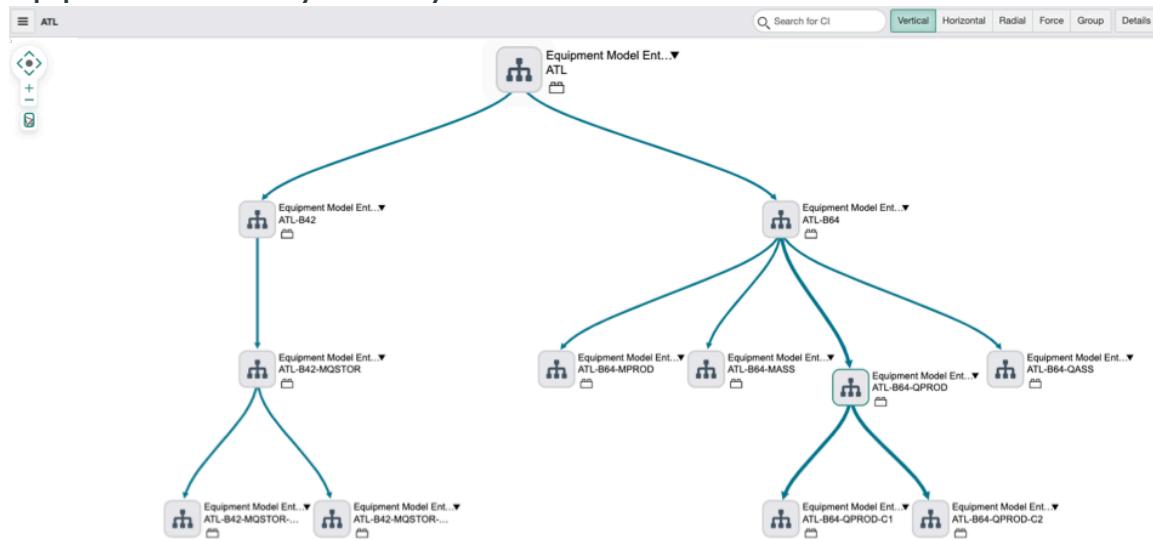
Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site you want to view equipment model information for.
You can search for a site by typing in the site name or its short code.
3. In the selector pane, click the equipment model entity you want to view a graphical representation of its hierarchy and relationship to other entities.
For example, click the top-level site entity to view a representation of the entire site.
4. To view the hierarchical structure for the equipment model entity, click **View hierarchy**.

Result

The following graphical representation appears For the selected equipment model entity. The currently selected equipment model appears as the parent entity in the hierarchy.

Equipment model entity hierarchy



View the equipment model OT device map

View the graphical representation of the selected equipment model entity and its relationship to other Operational Technology (OT) devices in the production process.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
2. In the **Equipment mode view for** field, select the site that you want to view equipment model information for.
You can search for a site by typing in the site name or its short code.
3. In the selector pane, select the equipment model entity you want to view a graphical representation of its relationship to other devices.
For example, select the top-level site entity to view a representation of the entire site.
4. To view the equipment model entity's relationships with devices, select **View OT Device Map**.

View the equipment model OT dependency map

View the graphical representation of the hierarchical structure of the selected equipment model entity and its relationship with other entities and devices in the production process.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
2. In the **Equipment mode view for** field, select the site that you want to view equipment model information for.
You can search for a site by typing in the site name or its short code.
3. In the selector pane, select the equipment model entity you want to view a graphical representation of its hierarchy and relationship to other devices and entities.
For example, select the top-level site entity to view a representation of the entire site.
4. To view the equipment model entity's hierarchical structure of relationships with other devices and entities, select **View OT Dependency map**.

Map the upstream production processes for the selected equipment model entity

Use the upstream process to review upstream production processes for the selected equipment model entity. You can also create and map a new upstream production process for the equipment model entity.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_viewer, cmdb_ot_isa_admin

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view equipment model information for.
You can search for a site by typing in the site name or its short code.
3. In the selector pane, expand the equipment model hierarchy and then click the entity that you want to view.
4. To view the upstream production processes for the equipment model entity, click **Upstream Process**.
5. Review the upstream production processes for the equipment model, or map a new one.

Task	Description
Review the upstream production processes for the selected equipment model entity	Proceed to the next step and review the Upstream process form.

Task	Description
Map an upstream production process	<p>a. Click Add.</p> <p>b. In the Map Upstream Process form, enter the name of the new production process entity that you are creating.</p> <p>c. Click Save.</p>
Remove an upstream process	<p>Use the Dependency Map view.</p> <p>a. Click View Process.</p> <p>b. Right-click the relationship that you want to delete.</p> <p>c. Click Delete Relationship.</p> <p>Use the upstream process record.</p> <p>a. Select the checkbox next to the upstream process you want to remove.</p> <p>b. Select Delete.</p> <p>c. In the confirmation message, select Confirm.</p>

6. Click **Submit**.

Map the downstream production processes for the selected equipment model entity

Use the downstream process to review the downstream production processes for the selected equipment model entity. You can also create and map a new downstream production process for the equipment model entity.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_viewer, cmdb_ot_isa_admin

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
You can search for a site by typing in the site name or its short code.
3. In the selector pane, expand the equipment model hierarchy and then click the entity that you want to view.
4. To view the downstream production processes for the equipment model entity, click **Downstream Process**.
5. Review the downstream production processes for the equipment model, or map a new one.

Task	Description
Review the downstream production processes for the selected equipment model entity	Proceed to the next step and review the Downstream process form.
Map a downstream production process	<ul style="list-style-type: none"> a. Click Add. b. In the Map Downstream Process form, enter the name of the new production process entity that you are creating. c. Click Save.
Remove a downstream process	<p>Use the Dependency Map view.</p> <ul style="list-style-type: none"> a. Click View Process. b. Right-click the relationship that you want to delete. c. Click Delete Relationship. <p>Use the downstream process record.</p> <ul style="list-style-type: none"> a. Select the checkbox next to the downstream process you want to remove. b. Select Delete. c. In the confirmation message, select Confirm.

6. Click **Submit**.

Review the child entities for the equipment model entity

Review the child entities that are associated with the selected equipment model entity. You can review the relationships of the associated entities that are subordinate to a higher-level entity.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Workspace**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
You can search for a site by typing in the site name or its short code.
3. In the selector pane, expand the equipment model hierarchy, and then click the entity that you want to view.
4. To view the child entities for the equipment model entity, click **Child Entities**.

- To create a new child entity, click the **Create new entity** button and fill in the details in the Create new entity form.
To learn more, see [Create an entity for a new equipment model](#).

Add OT devices that are associated with the selected equipment model entity

Use OT devices to review the OT devices that are associated with the selected equipment model entity and its child entities. You can also select and associate other OT devices to the selected equipment model entity.

Before you begin

To associate additional OT devices to the selected equipment model entity, both the Operational Technology Manager and Industrial Process Manager applications must be installed.

Role required: To add OT devices, the logged in user has to have a combination of the following assigned roles:

- cmdb_ot_viewer, cmdb_ot_editor or cmdb_ot_admin role
- cmdb_ot_isa_editor or cmdb_ot_isa_admin role

Note: To learn more about assigning user roles, see [Assign Industrial Process Manager user roles](#).

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see [Assign or remove equipment model site access for non-administrators](#).

Procedure

- Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Manager**.
You can search for a site by typing in the site name or its short code.
- In the **Equipment model view for** field, select the site you want to view equipment model information for.
- In the selector pane, expand the equipment model hierarchy, and then click the entity that you want to view.
- To view the associated OT devices for the equipment model entity and its child entities, click **Mapped OT Devices**.
- Review the associated OT devices or the associate additional OT devices to the selected equipment model entity.

Task	Description
Review the associated OT devices for the selected equipment model entity	Proceed to the next step and review the OT devices form.

Task	Description
Associate the additional OT devices to the selected equipment model entity	<p>a. Click Add.</p> <p>b. In the OT devices form, select the additional OT devices that you want to associate with the equipment model entity.</p> <p>c. Click Add to add them to the OT devices form.</p>
Remove the OT devices from the selected equipment model entity	<p>a. In the Mapped OT Devices list view, select the OT devices that you want to remove.</p> <p>b. Click Remove.</p>

6. Click **Save**.

Automated mapping of OT devices to the Equipment Model

Automate mapping of OT devices to the production process.

When OT managers experience vulnerabilities or need to manage workflow involving OT devices, the context of how the OT device connects to the production process it automates is critical to prioritizing work. Automatic mapping of OT devices to ISA equipment model entities enables the view of device-to-process relationships.

i Note: Only one subnet range per site is supported. Two different sites can have the same subnet; for example, 192.168.101.0/24. But multiple subnets of the same range are **not** supported for the same site. It is recommended that you use manual mapping in this scenario.

Key benefits

- Upload and store OT subnets from authoritative sources (such as NetDB or Firewalls) as records in a ServiceNow instance.
- Automate assignment of OT devices to ISA entity using IP addresses and OT subnet
- Minimize issues with reuse of private IP address ranges across multiple sites

Industrial networks use subnets to divide the private IP address space with a single subnet often aligned to a part of the production process, or the equipment model entity. For example: A canning line runs on a 192.168.101.0/24 network in which all the equipment was programmed by the integrator. The IPs used by the control systems, or OT devices, are often hard coded into the automation software used to run the line. If the subnet maps to the canning line in the Atlanta site, a manager can automatically map a detected PLC with IP 192.168.101.66 to the canning line.

The mapping feature relates each subnet to an equipment model entity, enabling you to automatically map OT devices to the subnets associated with the equipment model entity based on the IP address that was reported upon import from an OT Certified integration or ServiceNow® [Discovery for OT](#).

A system administrator can import OT subnet mapping records. An ISA administrator can automatically create mappings of subnets to equipment model entities through a scheduled job flow. An ISA Editor can manually create mappings of an individual OT device on-demand.

Automated mapping feature personas

The automated mapping feature is aimed at the following personas.

Persona	Description
System Admin	<p>The System admin performs these tasks:</p> <ul style="list-style-type: none"> Imports data into the OT subnet to Equipment Model Entity Mapping table Activates, schedules, or manually triggers the OT Subnet Mapping scheduled flow
ISA Admin	<p>The ISA admin manually triggers the Map all OT devices UI action from the OT Subnet Mapping list view.</p>
ISA Editor	<p>The ISA editor performs these tasks:</p> <ul style="list-style-type: none"> Manually creates and updates OT subnet mapping entries for specific sites Maps individual OT devices to an equipment model entity from an OT device record Maps multiple OT devices to an equipment model entity from an OT subnet mapping record

Plugins

Enabling the mapping feature requires the following plugins:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

If the required plugins are installed, an ISA administrator can access the subnet mapping feature from the Industrial Process Manager application menu.

Workflow for the automated mapping feature

The Industrial Process Manager includes an automated flow for the automated mapping feature.

A predefined flows is included with this feature that you can use to schedule the assignment of OT devices to equipment model entities.

By using [Flow Designer](#), you can review and configure the predefined flow for your business needs.

Flow available for this feature

The following table lists the predefined flow that is available with the Industrial Process Manager when installed with Operational Technology Manager.

Application	Flow
Industrial Process Manager when installed with Operational Technology Manager	OT device mapping flow

General use cases for the automated mapping feature

These use cases typically apply for the automated mapping feature:

- An OT manager has existing OT devices and wants to map individual OT devices on demand.
- An OT admin wants to automatically map newly detected OT devices with valid IP addresses to an equipment model entity.

The following is a typical workflow for the automated mapping feature.

- A system admin imports OT subnet data into the OT subnet mapping table from an Excel spreadsheet using [Easy Import](#).
- Either the Amazing admin reviews the imported data records and associates (maps) OT subnet mapping records to a site and/or the Equipment Model Entity within that site.
- The Amazing admin activates or triggers the scheduled flow to automatically map OT devices for all sites on an instance.
- The Amazing editor can update the records that belong to the sites that they have editing access to.

Configure Automated Mapping of OT devices using guided setup

Use the Industrial Process Manager guided setup to automatically map OT devices to the ISA equipment model entity.

Before you begin

Role required: admin

About this task

If you have the admin role, you can use the Industrial Process Manager Guided Setup to walk you through mapping OT devices to the ISA equipment model entity. You can map OT devices for the sites that you have access to.

Procedure

1. Navigate to **All > Industrial Workspace Admin > Guided Setup**.
2. Select **Get Started** for the Industrial Process Manager application.
3. Select the **Automatically Map OT Devices** task.
4. Select the following task tabs, then select **Configure** to complete the configuration tasks.

Task	Purpose
Import OT Subnets	Upload a spreadsheet of OT subnets to import subnets from network management platforms.
Add Sites	Add a site to each OT subnet so that OT devices with IP addresses matched with the OT

Task	Purpose
	subnet record can be mapped to that site automatically.
Add Equipment Model Entities	Add an equipment model entity to the OT subnet record to automatically associate an OT device with the equipment model entity.
Select Discovery Source(s)	Configure the following OT subnet-mapping system properties to limit the discovery sources that OT subnet mapping considers. <ul style="list-style-type: none"> ◦ sn_otsm.map_all_ot_devices.all_discovery_sources ◦ sn_otsm.map_all_ot_devices.discovery_sources
Test Mappings	Validate assigned mappings of individual OT devices, individual OT subnets, multiple selected OT subnets, or all active OT subnets.
Activate and Schedule	Activate the scheduled flows to run scheduled mapping of all OT devices regularly. There are two subflows that you can trigger individually: <ul style="list-style-type: none"> ◦ Subflow to assign sites to OT devices ◦ subflow to map OT devices to a site

Related topics

[Guided setup](#) 

[Automated mapping of OT devices to the Equipment Model](#)

Automatically map all OT devices to an equipment model entity

An Amazing admin can trigger automated mapping of all OT devices to the appropriate ISA equipment model entity.

Before you begin

The following plugins must be installed:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

Role required: sn_ot_amazing_admin

Procedure

1. Navigate to **Industrial Workspace Admin > Industrial Process Manager > OT Subnet Mapping**.
2. Select **Map all OT devices** to execute the Map OT Device flow.

Result

OT devices are automatically mapped to the Equipment Model Entities listed on all "active" OT subnet mapping records. After the mapping is triggered, you can view the mapping results by selecting the link available in the information message from the list view.

Map all OT devices within a subnet

An OT admin can trigger automated mapping of all OT devices within a selected subnet.

Before you begin

The following plugins must be installed:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

Role required: sn_ot_amazing_write

Procedure

1. Navigate to **Industrial Workspace Admin > Industrial Process Manager > OT Subnet Mapping**.
2. From the OT Subnet Mapping list, open the OT subnet mapping record whose devices you want to map.
3. Ensure that the Site and Equipment Model Entity fields are correctly completed.
4. Select the **Map OT devices in this subnet** UI Action to automatically map all OT devices in this site with IP addresses in the selected OT subnet.

Result

If there are OT devices in the selected site with IP addresses that fall in the selected IP range, all devices in the site are mapped for the OT subnet. After the mapping is triggered, you can view the mapping results by selecting the link available in the information message from the list view.

View OT devices not assigned to a site

View the list of Operational Technology (OT) devices that aren't assigned to a site.

Before you begin

The following plugins must be installed:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

Role required: cmdb_ot_isa_editor and cmdb_ot_editor

About this task

As part of OT device mapping, you need to assign the device to a site before mapping it to an equipment model entity. To do this, you can view a list of all the OT devices that aren't assigned to a site.

Procedure

1. Navigate to **All > Operational Technology (OT) > OT Devices w/o Site Assignment**.
2. To assign a device to a site individually, select the device record and updating the **Site** field.
3. To perform a bulk edit to update the **Site** column and assign multiple devices to the same site, complete the following steps.

- a. Select the check boxes next to each OT device you want to assign to a site.
- b. In the **Site** column header, select the Column options button and choose **Update Selected**.
- c. Update the **Site** field.
- d. Select **Update**.

What to do next

The OT devices are assigned to a site but not mapped to an equipment model entity. You can view a list of the unmapped OT devices to complete the device mapping. For more information, see [View unmapped OT devices](#).

View unmapped OT devices

View a list of Operational Technology (OT) devices with IP addresses that aren't mapped to any equipment model entity.

Before you begin

The following plugins must be installed:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

Role required: cmdb_ot_isa_editor and cmdb_ot_editor

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the Industrial Workspace list view under the **Operational Technology (OT)** module, select the **Unmapped OT Devices** list.
This list shows the OT device records with IP addresses and other fields that you can use to map them to equipment model entities for your assigned site.
3. Optional: In the **Site** column header, select the Filter button and choose **Group by Site**.
This filter lets you organize the unmapped OT devices by site and can be helpful if you manage multiple sites.

What to do next

Now, you can map the OT devices to equipment model entities. For more information, see [Map an individual OT device to an equipment model entity](#).

Map an individual OT device to an equipment model entity

Perform on-demand mapping of an OT device to the ISA equipment model entity for the sites that you have access to.

Before you begin

The following plugins must be installed:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

Role required: sn_ot_amazing_write and cmdb_ot_viewer

Procedure

1. Navigate to **All > Operational Technology (OT) > All OT Devices**.
2. In the **OT device** column, select the OT device that you want to map.
3. In the Related Links section, select **Map OT device**.

The screenshot shows a ServiceNow application window. At the top, there are buttons for 'Update' and 'Delete'. Below them is a 'Related Links' section with four items: 'Subscribe', 'Map OT asset' (which is highlighted with a blue border), 'Equipment Model Entities (1)', and 'Network Adapters (1)'. The main content area is titled 'OT Control Modules (4)' and contains a table with columns: Entity name, Short code, Path, Site, Template, Level, Type, Parent, Process criticality, Assigned to, Support group, and Managed By Group. A single row is visible: 'Production Line B' with 'PLB' as the short code, 'VEN-B01-PLB' as the path, 'Venus' as the site, '(empty)' as the template, '(empty)' as the level, '(empty)' as the type, 'VEN-B01' as the parent, '4 - not critical' as the process criticality, '(empty)' as the assigned to, '(empty)' as the support group, and '(empty)' as the managed by group. At the bottom of the table, it says '1 to 1 of 1'.

Result

If there is an active OT subnet that matches the IP address and site of the selected device, the device is mapped.

Configure the OT Subnet Mapping scheduled flow

Configure the OT device mapping flow to automatically map OT devices to sites and equipment model entities.

Before you begin

The following plugins must be installed:

- [Operational Technology Manager](#)
- [Industrial Process Manager](#)

Role required: admin

About this task

The OT device mapping flow can be set to run on a scheduled basis to automatically map OT devices for all active OT subnet mapping records.

Procedure

1. Navigate to **Industrial Workspace Admin > Industrial Process Manager > OT Subnet Mapping Scheduled Flow**.
2. Optional: Activate site mapping:
 - a. Open the Set Flow Variables section.
 - b. Check the box next to **Run Auto Assign Site** and select **Save**.
3. To schedule the flow to run on a regular basis, select the link in the Trigger section to define the interval.
4. In the header, select **Activate** to activate the scheduled execution of the OT device mapping flow.
After activation, this flow can run on a scheduled basis to automatically map OT devices for all active OT subnet mapping records on an instance.

View OT subnet mappings

View all mapped OT subnets assigned to an equipment model entity.

Before you begin

Roles required:

- sn_ot_amazing_write, cmdb_ot_isa_editor, and cmdb_ot_viewer or
- sn_ot_amazing_admin, cmdb_ot_isa_editor, and cmdb_ot_viewer

Procedure

1. Navigate to the Workspace using one of these options:
 - Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Equipment Model Workspace**.
 - Select the Industrial Workspace from the workspace menu item in the header.
2. From the Equipment model view, select the site, or expand the equipment model hierarchy to select the entity that you want to view mappings for.
3. In the entity form, select the **Mapped OT subnets** related list tab.
The mapped OT subnets show as active or inactive. Only active OT subnets will be included in the scheduled flow. For more information, see [Configure the OT Subnet Mapping scheduled flow](#).
4. Optional: To view the OT subnets that are used for mapping at the OT device level, select the **OT Subnets** related list in an OT device record.

What to do next

[Create a new OT subnet mapping record](#)

Create a new OT subnet mapping record

Create a new OT subnet mapping to associate with an equipment model entity.

Before you begin

Role required: sn_ot_amazing_write or sn_ot_amazing_admin

Note: When creating new OT subnet mapping records, by default the new records are inactive. To automatically map records when the OT device mapping flow triggers, OT subnet mapping records must be active.

Procedure

1. Navigate to **Industrial Workspace Admin > Industrial Process Manager > Equipment Model Entities**.
2. Select the site or equipment model entity you want to create a new mapping for.
3. Select the **Mapped OT Subnets** related list, then select **New**.
4. On the form, fill in the fields.

OT Subnet to Equipment Model Entity Mapping form

Field	Description
Name	Zone or VLAN name for the subnet.
Site	From the Lookup, select the ISA site from the list of available sites if not already populated.
Type	Select the subnet type from these options:

Field	Description
	<ul style="list-style-type: none"> IP Range - a subset of IP addresses in a subnet IP Network - the entire subnet, in CIDR notation
Starting IP Address	<p>Starting IP for the IP Range</p> <p>This field is visible when Type is IP Range.</p>
Ending IP address	<p>Ending IP for the IP Range</p> <p>This field is visible when Type is IP Range.</p>
Source name	Name of the source, such as NetDB or Firewall.
Firewall Name	Name of the firewall managing the zone if applicable.
Description	Description for the subnet mapping.
Active	Select Active to include the subnet in automated mapping when the OT Subnet Mapping scheduled flow executes.
Equipment model entity	From the Lookup, select the equipment model entity from the list of available entities if not already populated.
Subnet	Enter the subnet address (CIDR format). This field is visible when Type is IP Network.
Location	<p>Add a location to the subnet record to automatically add or update the location in the mapped OT devices.</p> <p>Note: The location is mapped based on the <code>sn_otsm.subnet_mapping.location_auto_update</code> system property. For more information about system properties used for OT subnet mapping, see System properties used by the OT subnet mapping feature.</p>
Interface name	Name for the firewall interface if applicable.
VLAN ID	Specify the VLAN ID if applicable.

5. Select **Submit**.

View all mapped OT devices

View a list of all the Operational Technology (OT) devices that are mapped to an equipment model entity.

Before you begin

Role required: sn_ot_amazing_write or sn_ot_amazing_admin

Procedure

Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Mapped OT Devices**.

This list contains all the devices that are mapped with different equipment model entities. The **Automates by :: Automates** CI relationship is applied to the parent and child entities.

System properties used by the OT subnet mapping feature

An Amazing Admin can view and configure the system properties that support the OT subnet mapping feature.

Users with the Amazing Admin role can access OT subnet mapping property settings by navigating to **Industrial Workspace Admin > Industrial Process Manager > OT Subnet Mapping Properties**.

OT subnet mapping system properties

Property	Description
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	Controls mapping of OT devices for all discovery sources. Map OT devices for all discovery sources. If checked, this will override the specific discovery sources below. Default is Yes (true). Default value: true
<code>sn_otsm.map_all_ot_assets.discovery_sources</code>	Maps OT devices for specified discovery sources (comma separated format). Only applicable if "Map OT devices for all discovery sources" above is unchecked.
<code>sn_otsm.subnet_mapping.auto_assign_ot_devices</code>	Automatically assigns all OT control modules to equipment model entities based on the Owns::Owned by relationship. Default is Yes (true).
<code>sn_otsm.subnet_mapping.location_auto_override</code>	Override location of an OT device with subnet's location. If checked, the location of the subnet takes precedence over OT device's location when it's mapped with the subnet. Default is Yes.

Automated mapping components installed when Industrial Process Manager and Operational Technology Manager are both installed

Several types of automated mapping components will be installed with activation of the Industrial Process Manager when Operational Technology Manager is also active, including tables, system properties, and scheduled flows.

These automated mapping components are installed with or available when Industrial Process Manager is installed with Operational Technology Manager.

Tables

Table	Description
OT Subnet to Equipment Model Entity Mapping [ot_subnet_mapping]	Stores the mappings of OT subnet to equipment model entities.

Properties

Property	Description
sn_otsm.map_all_ot_assets.all_discovery_sources	Control mapping of OT devices for all discovery sources. Default value: true
sn_otsm.map_all_ot_assets.discovery_sources	Map OT devices for specified discovery sources (comma separated format).
sn_otsm.subnet_mapping.auto_assign_ot_control_modules	Automatically assigns all OT control modules to equipment model entities based on the Owns::Owned by relationship. Default is Yes (true).
sn_otsm.subnet_mapping.location_auto_update	Override location of an OT device with subnet's location. If checked, the location of the subnet takes precedence over OT device's location when it's mapped with the subnet. Default is Yes.

Flow Designer flows

Application	Flow
Industrial Process Manager integration with Operational Technology Manager	OT device mapping flow

Industrial Process Manager reference

Reference topics provide additional information about the Industrial Process Manager application.

Related information

For more information about the Operational Technology (OT) product view related to the Common Service Data Model (CSDM), the Network Intrusion Detection System (NIDS), OT extension classes, and related applications see the following.

Overview

The product view and the extension classes help you understand how Operational Technology Management works with the CSDM framework and the Configuration Management Database (CMDB) respectively.

[Operational Technology product view](#)

The Operational Technology product view helps you understand how Operational Technology key entities work with the CSDM framework.

[Network Intrusion Detection System \(NIDS\) CI extension class](#)

The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.

[Operational Technology \(OT\) extension classes](#)

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

[Operational Technology Manager](#)

The Operational Technology Manager application enables you to aggregate OT device data from multiple sources, so that you can build the foundational data relationships used in the Industrial solution.

Migrating site user access to user criteria and groups

When you upgrade to version 1.0.12 of the ISA Equipment Model, the migration from site user access to user criteria and groups begins automatically.

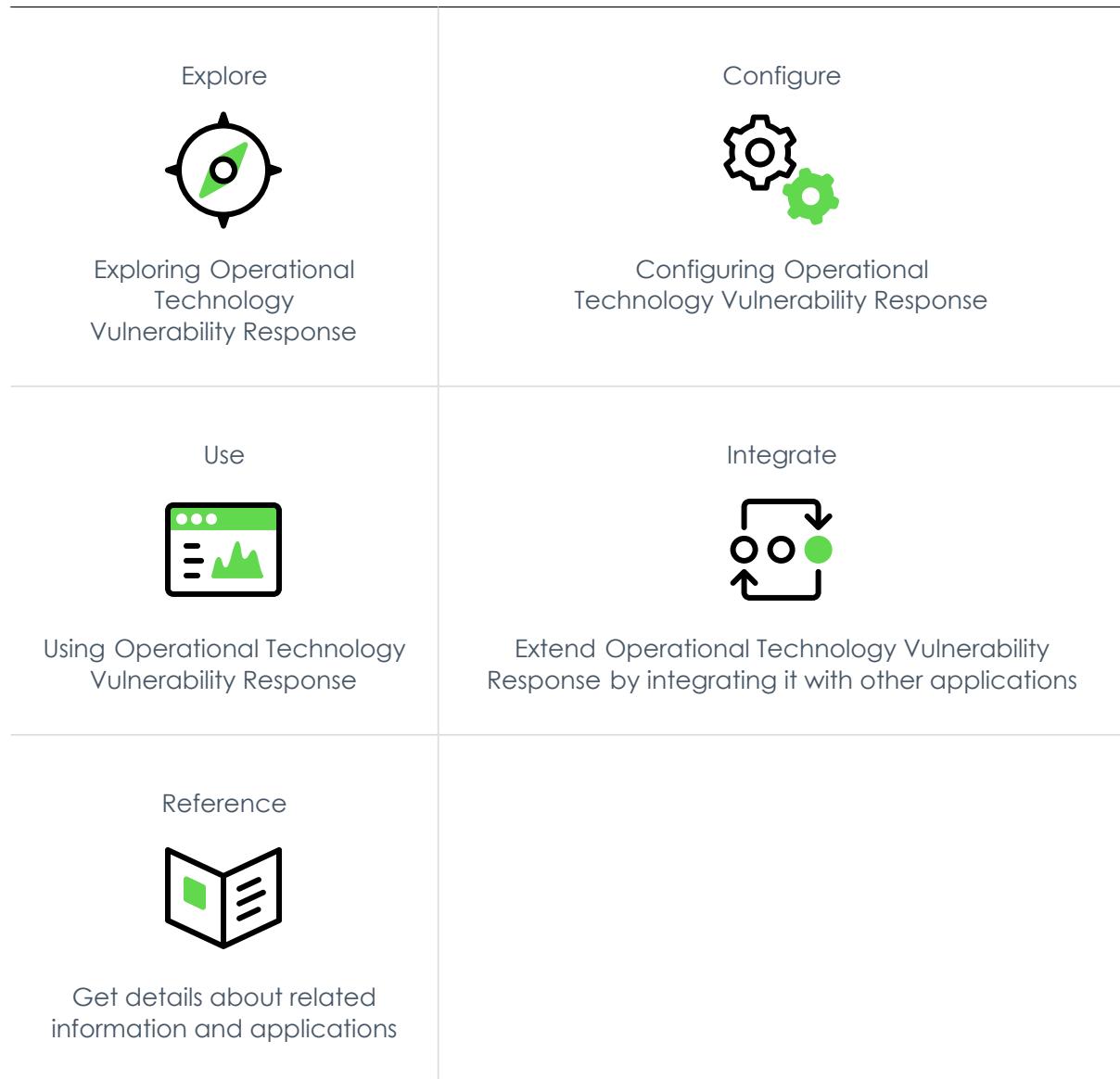
The following changes occur when you upgrade to version 1.0.12 of the ISA Equipment Model.

- Improved site level access control to that uses user criteria to define read or write level user access to equipment model entity sites. With the additional assignment of OT viewer (cmdb_ot_viewer) or OT Editor (cmdb_ot_editor) roles, you can also have view or edit access to OT devices in the sites assigned accordingly.
- When you upgrade to version 1.0.12 of ISA Equipment Model, existing site user records are migrated to an improved access control model using user criteria to preserve the same access permissions. For each site with ISA Entity Site User records, the following changes occur.
 - For users with viewer access:
 - A new user criteria record is created and named **Read User Criteria for <site name> Site#[System Generated]**
 - A new user group with all site users from this site is created and named **Read Group for <site name> Site [System Generated]**
 - A new record in the new Equipment Model Entity View Access table (isa_entity_m2m_user_criteria_can_view) is created with the new user criteria and user group.
 - For users with editor access:
 - A new user criteria record is created and named **Edit User Criteria for <site name> Site [System Generated]**
 - A new user group with all site users from this site is created and named **Edit Group for <site name> Site [System Generated]**
 - A new record in the new Equipment Model Entity Edit Access table (isa_entity_m2m_user_criteria_can_edit) is created with the new user criteria and user group.
- The Site User application menu and Site Users related list on the Equipment Model Entity record for a site is removed.
- All site user (isa_entity_site_user) records are set to inactive.

- The **Site User – Can Read** and **Site User – Can Edit** application menu items are added to the Now Platform.
- The **Can Read Equipment Models** and **Can Edit Equipment Models** related lists are added to the Equipment Model Entity record for a site.

Operational Technology Vulnerability Response

Operational Technology Vulnerability Response enables effective prioritization and remediation of OT device vulnerabilities at the site level. By leveraging the CMDB relationships of OT devices, vulnerable devices or items can be prioritized based on the criticality of the production process they automate.



Exploring Operational Technology Vulnerability Response

Use Operational Technology Vulnerability Response as an integrated solution for the industrial production process.

As an OT engineer or OT vulnerability manager, Operational Technology Vulnerability Response enables you to find answers to the questions such as:

- What are my OT device vulnerabilities?
- How can I prioritize vulnerability remediation using OT specific risk?
- What progress are we making toward remediating OT vulnerabilities?

Remediation task and vulnerable item states

Vulnerable items (VIs) and their remediation tasks can have different states due to complex use cases. For more information about remediation task and vulnerable item states and their workflow, see [Vulnerability Response remediation task and vulnerable item states](#).

Key features

With Operational Technology Vulnerability Response, you can use the following key features.

- The OT Vulnerabilities landing page is a centralized location in the Industrial Workspace that enables you to review your data from the Operational Technology Vulnerability Response application.
- The Operational Technology Vulnerability Response (PA) dashboard tracks the volume, performance, and progress of OT VIs from initial analysis and detection to containment, or remediation.

Operational Technology Vulnerabilities landing page tab

The Operational Technology (OT) Vulnerabilities landing page tab is a centralized location in the Industrial Workspace that enables you to review your data from the Operational Technology Vulnerability Response application. You use it to review or edit detailed information for the OT vulnerabilities in your OT network.

Note: The OT Vulnerabilities landing page tab is included in the entitlement with the Operational Technology Manager application and runs in Performance Analytics. But an additional license for Performance Analytics is not required. However, if you want to create new indicators, you need the Performance Analytics - Premium plugin. For more information, see [Activating your Performance Analytics subscription](#).

The OT Vulnerabilities landing page tab lets you view the following:

- Number of new OT vulnerable items
- Vulnerable items that have not been addressed
- Vulnerable items organized by state
- Vulnerable items organized by their risk rating
- Vulnerability risk table that shows your existing equipment model entities, vulnerable items, and risk scores

Landing page tab contents

To access the OT Vulnerabilities landing page tab, navigate to **All > Industrial Workspace**, select the Home () icon, and then select the **OT Vulnerabilities** tab. To access the KPI graph for a tile, select the number count or chart component in the tile.

This table describes the information that you see and can review in the OT Vulnerabilities landing page tab.

OT Vulnerabilities landing page tab

Title	Description
OT vulnerabilities overview	<p>Section that contains your OT vulnerability data.</p> <p>i Note: If the job ran successfully, there's a Last updated: timestamp that indicated the end time of the last collection. If the job is unsuccessful, there's a Last executed timestamp that indicates the end time of the last execution.</p>
New OT vulnerable items	Total number of new OT vulnerable items found in your system.
Unaddressed vulnerable items	Total number of OT vulnerable items that are open and haven't been assigned to a user.
Vulnerable Items by Risk Rating	Circle chart that summarizes your vulnerable items and their criticality.
Vulnerable items by state	Bar chart that displays all the vulnerable items by state. You can interpret how many vulnerabilities are being addressed and how many need further investigation. For example, if the Under Investigation category is relatively high, you can prioritize these items by addressing those vulnerable items first.
Vulnerability risk	Table that displays the risk scores for your site's equipment model entities and their vulnerable items. It also highlights the area that poses the most risk.

OT landing page filters

The OT landing page offers filters to specify the data you see on your landing page at a per-site and business unit level.

Business unit filter

The business unit (BU) filter lets you do the following:

- View OT data for all business units.
- View OT data for a specific business unit.
- View OT data for multiple business units.

By default, the landing page shows OT data for all of your available BUs as shown in the following image.

The screenshot shows the ServiceNow OT Manager landing page. At the top, there's a navigation bar with links for All, Favorites, History, Workspaces, Admin, and Industrial Workspace. Below the navigation bar, a message says "Hello System, welcome to OT Manager!". Underneath this, there are two dropdown menus: "All business units" and "All sites". The "All business units" dropdown is highlighted with a red box.

To view OT data for one or more BUs, do these actions:

1. Select the **All business units** drop-down on the landing page header.
2. From the list, select one or more BUs that you want to see data for. You can use the search function to search for a specific BU.

Once you set the BU filter, the landing page displays data from every site included in the selected BUs. You can then choose a site from the **All Sites** drop-down, described in the next section. If you change the BU filter and select different BUs, the site filter is updated to only include sites associated with the new BU selection.

Site filter

The site filter lets you do the following:

- View OT data for all sites.
- View OT data for a specific site.
- View OT data for multiple sites.
- View OT data for no site assigned.

Note: If there's no site assigned to an OT device, the filter shows **No site assigned**.

To have the correct sites shown on the landing page, you must assign a site to the device and then assign a business unit to that site.

By default, the landing page shows OT data for all sites as shown in the following image.

The screenshot shows the ServiceNow OT Manager landing page. At the top, there's a navigation bar with links for All, Favorites, History, Workspaces, Admin, and Industrial Workspace. Below the navigation bar, a message says "Hello System, welcome to OT Manager!". Underneath this, there are two dropdown menus: "All business units" and "All sites". The "All sites" dropdown is highlighted with a red box.

To view OT data for one or more sites, do these actions:

1. Select the **All sites** drop-down on the landing page header.
2. From the list, select one or more sites that you want to see data for.

Note: You can use the search function to search for a specific site. Type the name of the site or the short code in the search bar.

Setting up the OT Vulnerabilities landing page tab

Complete the Guided Setup tasks to set up the OT Vulnerabilities landing page tab with the correct data collections, indicator resources, and filters.

For more information about the OT Vulnerabilities landing page tab and its contents, see [Operational Technology Vulnerabilities landing page tab](#).

OT Vulnerabilities landing page tab Guided Setup tasks

Task	Purpose
Complete the OT Vulnerabilities Data Collection Configuration.	Collects and displays daily data for all indicators from Performance Analytics for the OT Vulnerabilities landing page tab. You must complete this step before others can view the landing page tab.
[Optional] Review the indicator sources.	By default, each indicator of the OT Vulnerabilities landing page tab can only show 1 million records. If you expect more than 1 million total records, you must override the records collection.

Configure the data collection for OT vulnerable items

Configure the data collection for Operational Technology (OT) vulnerable items (VIs) to collect and display daily data for all indicators from Performance Analytics.

Before you begin

Role required: admin

About this task

When the OT Vulnerable Items Daily Data Collection job hasn't run yet, no data is available for the landing page tab and the **Last updated** timestamp is hidden. If you're an admin, you see the following error message that prompts you to run the OT Vulnerable Items Daily Data Collection

job:

- Note:** If you're not an admin, the error message prompts you to reach out to the admin for further assistance.

To run the OT Vulnerable Items Daily Data Collection job, complete the following steps.

Procedure

1. Navigate to All > Data Collector > Performance Analytics > Jobs.

Alternatively, if you're in the OT Vulnerabilities landing page tab, select **Run job now** in the error message.

2. Select the Show / hide filter () icon and apply a filter of [Name] [is] [OT Vulnerable Items Daily Data Collection].

3. Select the check box next to the **Active** field under the **Job parameters** section and schedule a time in the **Run** field to start collecting data.

Alternatively, you can use the **Execute Now** button to collect data manually. Otherwise, no data is shown when you view the landing page tab. It's recommended to only use the **Execute Now** button when you first run the job. Everyday data collected after this point should be collected at a scheduled time.

4. Check if the default schedule collection time works for you.

The default time is 00:00:00 daily. If you want to change the default collection time, you can change it after activating the job. Please notify users of this change.

Result

The OT Vulnerabilities landing page tab now displays the correct data for the collected OT vulnerable items for your users.

Review the indicator sources

Review the indicator sources if a larger number of records is needed, so that the landing page tab can show more records than the default value of 1 million and the error message is cleared.

Before you begin

Role required: admin

About this task

Due to the migration with Performance Analytics, each indicator of the OT Vulnerabilities landing page tab can only show 1 million records by default. If you're an admin and records exceed 1 million after running the OT Vulnerable Items Daily Data Collection job, you see an error message that directs you to the job logs.

- i Note:** If you're not an admin and the records exceed 1 million after running the OT Vulnerable Items Daily Data Collection job, the error message appears directs you to the admin for help.

As an admin, you can check the job logs related list from the link in the error message and filter out the information to see which indicator source has the error. After you find the indicator source with the error, you can change the indicator sources for a larger number of records. This helps ensure that the indicator source data can be overridden, an error message no longer appears for other users, and data is shown for the indicator source. For more information about indicator sources, see [Indicator sources](#).

- i Note:** There may be warnings included in the job logs that aren't about the indicator sources. You must filter the job logs record by the **Level** column and find the error messages about indicator sources.

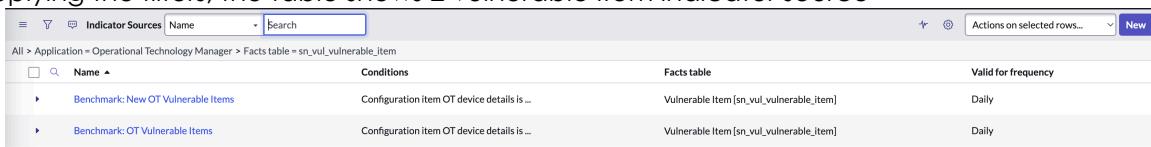
Procedure

1. Navigate to **All > Performance Analytics > Sources > Indicator Sources**.

2. Select the Show / hide filter () icon and apply the following filters.

- [Application] [is] [Operational Technology Manager]
- [Facts table] [is] [sn_vul_vulnerable_item]

After applying the filters, the table shows 2 vulnerable item indicator source



Name	Conditions	Facts table	Valid for frequency
Benchmark: New OT Vulnerable Items	Configuration item OT device details is ...	Vulnerable Item [sn_vul_vulnerable_item]	Daily
Benchmark: OT Vulnerable Items	Configuration item OT device details is ...	Vulnerable Item [sn_vul_vulnerable_item]	Daily

records.

3. Select the indicator source record that you need to change.

You can find which indicator source needs to be adjusted from job logs link in the error message.

4. In the Records Collection tab, select the check box next to the **Override records collection** field.

The **Maximum number of fetched records** field appears.

5. In the **Maximum number of fetched records** field, change the value to **xM**.

6. Select **Update**.

Operational Technology Vulnerability Response (PA) dashboard

Track the volume, performance, and progress of Operational Technology (OT) vulnerable items (VIs) from initial analysis and detection to containment, or remediation. You can filter reports by assignment group, exploits, risk rating, or state, for example. Quickly gain insight into your vulnerability exposure and which services are affected.

Required Operational Technology and Operational Technology Vulnerability Response roles

Role required: cmdb_ot_viewer, cmdb_ot_isa_viewer_all, and sn_vul.remediation_owner

Use cases

For examples of how different people in your organization can use this dashboard, see these use cases.

Operational Technology Vulnerability Response (PA) dashboard use cases

User	Dashboard use
OT site managers, OT analysts, vulnerability remediation owners	Help your organization deal with increasing security incidents due to exploited vulnerabilities by efficiently determining which OT vulnerable items present the most risk. This dashboard provides a graphical view into OT vulnerable item activity and help design remediation plans and status progress. You can focus on the KPIs associated with critical affected devices and high-visibility vulnerabilities.

To view the Operational Technology Vulnerability Response (PA) dashboard, navigate to **All > Industrial Workspace** and select the **dashboards** () icon on the left navigation panel.

See reports that show trending data over time. Reports with real-time data are listed below. View trends of important metrics on a regular schedule to analyze your overall business processes and identify areas of improvement.

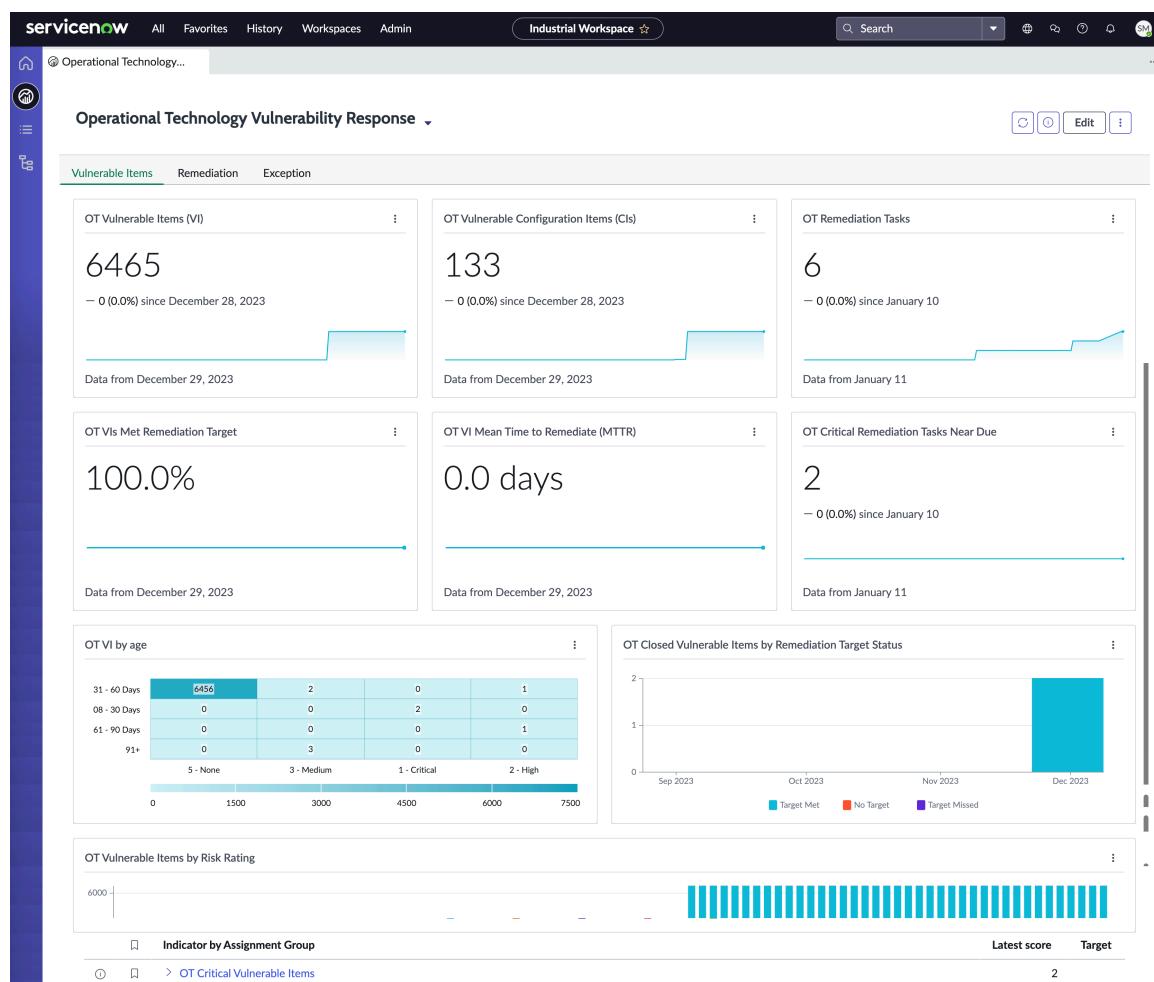
Operational Technology Vulnerability Response (PA) dashboard tabs

Vulnerable Items

This tab communicates KPIs for vulnerability risk and prevalence, affected devices, remediation target adherence, and remediation progress.

On the Vulnerable Items tab, you can view the following reports that are run based on the scheduled job:

- OT Vulnerable Items (VI)
- OT Vulnerable Configuration Items (CIs)
- OT Remediation Tasks
- OT VIs Met Remediation Target
- OT VI Mean Time to Remediate (MTTR)
- OT Critical Remediation Tasks Near Due
- OT VI by age
- OT Closed Vulnerable Items by Remediation Target Status
- OT Vulnerable Items by Risk Rating
- OT Critical Vulnerable Items by Assignment Group
- OT Overdue Critical Vulnerable Items by Assignment Group

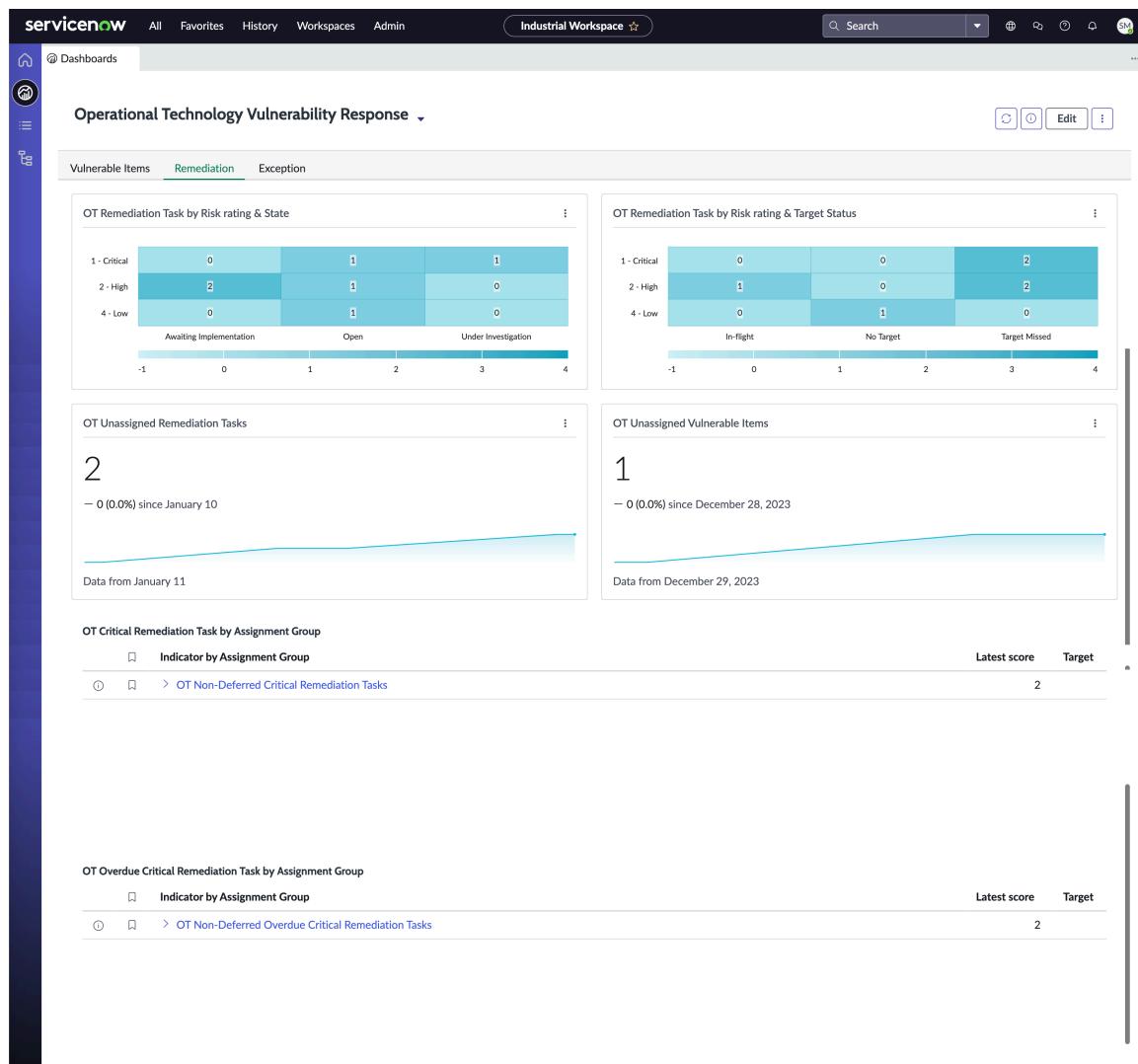


Remediation

This tab helps you understand the progress of your remediation actions, and which support teams need the most assistance with their completion.

On the Remediation tab, you can view the following reports in real-time:

- OT Remediation Task by Risk Rating & State
- OT Remediation by Risk Rating & Target Status
- OT Unassigned Remediation Tasks
- OT Unassigned Vulnerable Items
- OT Critical Remediation Task by Assignment Group
- OT Overdue Critical Remediation Task by Assignment Group

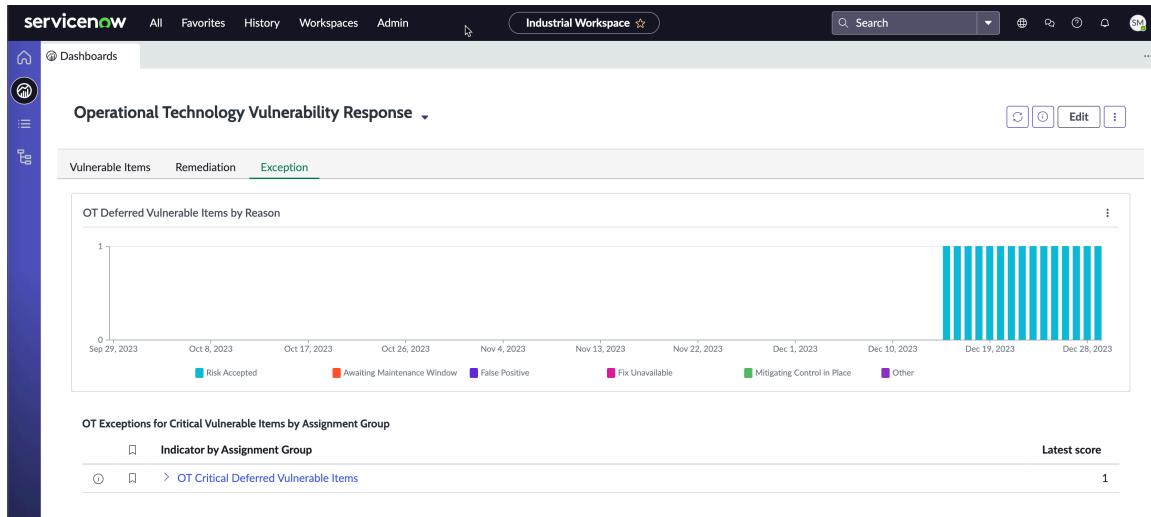


Exception

This tab helps you understand where your organization is taking risk due to potentially excessive deferrals and reconsider remediation options.

On the Exception tab, you can view the following reports in real-time:

- OT Deferred Vulnerable Items by Reason
- OT Exceptions for Critical Vulnerable Items by Assignment Group.



Indicator sources

Operational Technology Vulnerability Response indicator sources

There are 3 indicator sources that the Operational Technology Vulnerability Response indicators gather data from. If you expect more than 1 million records to be collected from the indicator sources, you must override the expected count in the **Records collection** section of the indicator source.

To do this, complete the following steps:

1. Navigate to **All > Performance Analytics > Sources > Indicator Sources**.
2. Apply the filter **[Application] [is] [Operational Technology Vulnerability Response]**.
3. Select the indicator source record.
4. Under the **Records collection** section, select the check box next to the **Override record collection** field.
5. Provide a number in the **Maximum number of fetched records** field. For example, **2 million**.

OTVI.Active

Uses the `sn_vul_vulnerable_item` table and includes all active vulnerable items in your OT system.

OTVI.Closed

Uses the `sn_vul_vulnerable_item` table and includes all the closed vulnerable items in your OT system.

OTRT.Active

Uses the sn_vul_vulnerability table and includes all the active remediation tasks in your OT system.

Indicators

Operational Technology Vulnerability Response indicators

There are a number of indicators used to measure and track the progress of your vulnerability remediation in the Operational Technology Vulnerability Response application.

The **collect records** option for the indicators is disabled by default for the Operational Technology Vulnerability Response application. This option is disabled to avoid the performance issues that may occur when you collect a large amount of data for each indicator.

OT Vulnerable Items

It is the count on data source OTVI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

OT Critical Vulnerable Items

It is the count on data source OTVI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

OT Unassigned Vulnerable Items

All active OT Vulnerable Items where both the Assignment Group and Assigned To fields are empty. Goal is to minimize.

OT Closed Vulnerable Items

OT Closed Vulnerable Items is measured daily as unit #. The goal is to maximize.

OT Deferred Vulnerable Items

It is the count on data source OTVI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

OT Critical Deferred Vulnerable Items

It is the count on data source OTVI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

OT Non-Deferred Overdue Critical Vulnerable Items

It is the count on data source OTVI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

OT Remediation Tasks

It is the count on data source OTRT.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

OT Non-Deferred Overdue Critical Remediation Tasks

It is the count on data source OTRT.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

OT Non-Deferred Remediation Tasks

It is the count on data source OTRT.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

OT Non-Deferred Critical Remediation Tasks

It is the count on data source OTRT.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

OT Unassigned Remediation Tasks

All active remediation tasks where both the Assignment Group and Assigned To fields are empty. Goal is to minimize.

% Vulnerable Items Met Remediation Target

```
([[Closed Vulnerable Items > Remediation Target = Target Met]] /  
[[Closed Vulnerable Items]]) * 100
```

. Goal is to maximize.

OT Vulnerable Item Mean Time to Remediate

```
[Summed Duration of Closed Vulnerable Items] / [[Closed  
Vulnerable Items]]
```

OT Summed Duration of Closed Vulnerable Items

It is the sum on data source OTVI.Closed, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

OT Vulnerable Configuration Items

It is the count distinct on data source OTVI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Breakdowns

The following breakdown names apply to the indicators on the dashboard:

- Age
- Age Closed
- Assignment Group
- CI Manager
- Deferral Reason
- Exploit Attack Vector
- Exploit Exists
- Exploit Skill Level
- Remediation Target Rule
- Remediation Target Status
- Remediation Target Status (Closed)
- Risk Rating
- Severity
- State

Breakdown source:

- Assignment Group
- Deferred.Reason.Non.Closed
- Exploit Attack Vector
- Exploit Exists
- Exploit Skill Level
- OT Age Range
- Remediation Target Status

- Remediation Target Status (Closed)
- Remediation.Target.Rule
- Risk Rating
- Severity
- State
- Vulnerable.Item.Cl.Manager

Collection jobs:

- [PA OT VR] Historical Vulnerability Data Collection

i Note: The Historical Vulnerability Data Collection is an on-demand job that you only need to execute once at the start. Once the historical data is collected, the daily data collection jobs run on a scheduled time every day. For more information, see [Collect historical data](#).

- [PA OT VR] Daily Collection for Remediation Tasks
- [PA OT VR] Daily Collection for Vulnerable Items 1
- [PA OT VR] Daily Collection for Vulnerable Items 2
- [PA OT VR] Daily Collection for Vulnerable Configuration Items (CIs)

Data visualizations

Vulnerable Items tab data visualizations

Name	Type	Description
OT Vulnerable Items (VI)	Single score	Number of active (non-closed) OT vulnerable items.
OT Vulnerable Configuration Items (CI)	Single score	Number of configuration items (CIs) associated with one or more active OT vulnerable items.
OT Remediation Tasks	Single score	Number of active (non-closed) OT remediation tasks.
OT VIs Met Remediation Target	Singe score	<p>Percentage of closed OT vulnerable items that have met their remediation target dates in the current and previous quarters.</p> <p>Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments).</p>
OT VI Mean Time to Remediate (MTTR)	Single score	The mean time to remediate (close) an OT vulnerable item, displayed as a 30-day running average.

Vulnerable Items tab data visualizations (continued)

Name	Type	Description
		<p>i Note: The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.</p>
OT Critical Remediation Tasks Near Due	Single score	<p>Number of active OT remediation tasks approaching their remediation target date.</p> <p>The remediation target date of an OT remediation task is set to the closest due date belonging to an active vulnerable item in the group.</p> <p>Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments).</p> <p>This report excludes deferred OT remediation tasks.</p>
OT VI by age	Heat map	Number of OT active vulnerable items grouped by age (in days).
OT Closed Vulnerable Items by Remediation Target Status	Bar	<p>Number of Closed OT vulnerable items grouped by remediation target status over the selected time span.</p> <p>i Note: The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.</p>
OT Vulnerable Items by Risk Rating	Bar	Number of active OT vulnerable items grouped by risk rating over the selected time span.

Remediation tab data visualizations

Name	Type	Description
OT Remediation Task by Risk rating & State	Heat map	Number of active OT remediation tasks grouped by risk rating and state.
OT Remediation Task by Risk rating & Target Status	Heat map	Number of active OT remediation tasks grouped by risk rating and remediation target status. This report excludes deferred OT vulnerable items.
OT Unassigned Remediation Tasks	Single score	Number of active OT remediation tasks without an assignee or assignment group.
OT Unassigned Vulnerable Items	Single score	Number of active OT vulnerable items without an assignee or assignment group.

Exception tab data visualizations

Name	Type	Description
OT Deferred Vulnerable Items by Reason	Bar	Number of deferred OT vulnerable items grouped by deferral reason.

Configuring Operational Technology Vulnerability Response

Configure operational technology (OT) assignment rules, remediation targets, risk calculators, and risk rollup calculation then configure integrations to create vulnerable item records.

***i* Note:**

If you have the admin role, you can use the Industrial Guided Setup to lead you through the setup of the Operational Technology Vulnerability Response application.

To access the Guided Setup, navigate to **Industrial Workspace Admin > Guided Setup**.

Task	Purpose
1. Install Operational Technology Vulnerability Response from the ServiceNow Store.	Install the Operational Technology Vulnerability Response application.
2. Assign roles to admin users# or user groups, if needed.	Assigns roles to control the actions that are available for each user.
3. Assign roles for the OT Vulnerability Remediation Owner.	Assigns roles to control the actions that are available for the OT Vulnerability Remediation Owner.

Task	Purpose
<p>4. Create assignment groups and assign users to sites and groups.</p> <p>1. Create an Operational Technology Vulnerability Response site assignment group for each site that you have in the Equipment Model Manager.</p> <p>2. Assign users who already have either the cmdb_ot_isa_viewer or cmdb_ot_isa_editor role to sites.</p> <p>3. Add users to the assignment group for their site.</p>	<ul style="list-style-type: none"> Allows OT Remediation Owner users to see only vulnerable items for their site. Allows users to see the Vulnerability Items for the sites they're assigned to.
<p>5. Configure OT remediation target rules.</p>	<ul style="list-style-type: none"> Assigns OT vulnerable items to site-level groups, or groups based on classification. Defines the expected timeframe for remediating vulnerable items.
<p>6. Load the demo data records for the Operational Technology Vulnerability Response application.</p>	Calculates the remediation target for OT vulnerable items.
<p>7. Configure OT risk calculators.</p>	Determines which OT risk factors to use when calculating the risk of a vulnerable item on an OT device.
<p>8. Configure OT risk roll up calculator.</p>	Calculates the risk score of the OT devices at each level for the equipment model entity.
<p>9. Install Operational Technology Certified integrations for the Operational Technology Vulnerability Response application that are applicable to your environment.</p>	Integrates certified third-party applications that enhance functionality of OT vulnerability management.

Install Operational Technology Vulnerability Response

Install the Operational Technology Vulnerability Response application if you have the admin role. This application includes demo data and installs the related store applications and plugins if they are not already installed.

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](#).
- If the application requires plugins or other store applications, install them first if they are not already installed.
- Operational Technology Vulnerability Response requires the following plugins. Ensure that these plugins are activated before you install Operational Technology Vulnerability Response.

Required ServiceNow plugins

Vulnerability Response (sn_vul)

The ServiceNow® Vulnerability Response application imports and automatically groups vulnerable items according to group rules allowing you to remediate vulnerabilities. See [Install Vulnerability Response](#).

Industrial Process Manager (sn_otsm)

Creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Industrial solution. See [Install the Industrial Process Manager](#).

Operational Technology Manager

The Operational Technology Manager application creates the foundational data and relationships that enable your enterprise to use the ServiceNow® Industrial solution. Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the Now Platform. See [Configuring the Operational Technology Manager \(OTM\)](#).

Role required: admin

About this task

The following items are installed with the installation of the Operational Technology Vulnerability Response application:

- Plugins
- Store applications
- Roles
- Business rules

For more information on viewing the components that are installed with an application, see the following:

- [Components installed with Operational Technology Vulnerability Response](#)
- [Find components installed with an application](#).

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Operational Technology Vulnerability Response application using the filter criteria and search bar.

You can search for the application by its name or ID. If you cannot find an 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. Select a version from the list and select **Install**.

In the Install dialog box that is displayed, any dependencies that are installed along with your application are listed.

4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. Optional: If demo data is available and you want to install it, select the **Load demo data** check box.
Demo data comprises the sample records that describe application features for the common use cases. Load the 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.

6. Select **Install**.

Components installed with Operational Technology Vulnerability Response

Several types of components are installed with activation of the Operational Technology Vulnerability Response (com.sn_otvr) plugin, including user roles and a business rule.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see [Find components installed with an application](#).

Demo data is available for this feature.

Roles installed

Role title [name]	Description	Contains roles
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view Operational Technology Vulnerability Response integration records.	None
OT VR Integration Admin [sn_otvr.integration_admin]	Can view and edit Operational Technology Vulnerability Response integration records.	<ul style="list-style-type: none"> • sn_sec_cmn.admin • sn_otvr.integration_viewer • sn_vul.read_all

Business rules installed

Business rule	Table	Description
Associate OT VITs To Remediation Task	Remediation Task [sn_vul_vulnerability]	When an OT Remediation task is created, groups the associated vulnerable items to the task with respect to the filter condition specified in the task->Filter grouping configuration.

Assign Operational Technology Vulnerability Response roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Operational Technology Vulnerability Response application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following tables can use the Operational Technology Vulnerability Response application.

Assign roles to admin users# or user groups as needed.

Assign roles to admin users# or groups

Role	Description
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view OT VR integration records.
OT VR Integration Admin [sn_otvr.integration_admin]	Can view and edit OT VR integration records.

Add the following roles to users who remediate OT vulnerable items in the Industrial Workspace.

Assign roles for the OT Vulnerability Remediation Owner

Role	Description
OT viewer [cmdb_ot_viewer]	Minimum role to read OT device records.
OT ISA viewer [cmdb_ot_isa_viewer]	Minimum role to view assigned Equipment Model Entity records. The user must also be assigned to any sites that they need to access records for.
VR Remediation Owner [sn_vul.remediation_owner]	Can read and edit vulnerable items records. Can view activity history on remediation task. Can add and view history of notes.
VR Close [sn_vul.close_vi_vg]	Can manually close Vulnerable Item records.

In addition to the OT Vulnerability Remediation Owner roles, add the following roles for users who group OT vulnerable items for remediation by equipment model entity in the Industrial Workspace.

Assign roles for the OT Vulnerability Remediation Task User

Role	Description
VR Remediation Owner [sn_vul.remediation_owner]	Can access remediation task list views. Can do split task functionality.
Remediation Task Manager [sn_vul.write_all]	Can update all vulnerable items and remediation tasks.

Assign roles for the OT Vulnerability Remediation Task User (continued)

Role	Description
VR Close [sn_vul.close_vi_vg]	Can close remediation tasks.

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

What to do next

[Create a site assignment group.](#)

Create a site assignment group

Create one Operational Technology Vulnerability Response assignment group per site that you have in the Equipment Model Manager. This allows OT Remediation Owner users to only see vulnerable items for their site.

Before you begin

Create an Operational Technology Vulnerability Response assignment group, preferably with the same name as the site it will be related to. For example, if your site is in Milan, name the group the 'Milan OT VR Assignment Group'.

Role required: cmdb_ot_isa_admin or admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Industrial Process Manager > Sites**.
2. Select a site record.
The site record is a parent Equipment Model Entity that has no parent itself.
3. In the **OT VR assignment group** field, select the search icon to show existing user groups.
4. Select the applicable assignment group.
 - If the desired group exists, select it from the list.
 - If the desired group does not exist, select **New** to create the group, then select **Submit**.
5. After returning to the site record, select **Update**.
The new OT VR assignment group is created.

What to do next

[Assign users to sites](#)

Assign users to sites

If you have not already done so during configuration of the Industrial Process Manager, assign users who already have either the cmdb_ot_isa_viewer or cmdb_ot_isa_editor role to sites.

Before you begin

When OT devices are in the CMDB, site access can be configured to limit visibility of OT devices to users with both a cmdb_ot_viewer, editor, or admin role, and a cmdb_ot_isa_viewer or editor role.

Role required: cmdb_ot_isa_admin or admin

Procedure

1. From the Equipment Model Entities form, select a parent Equipment Model entity. For information about equipment models, see [Managing equipment models](#).
2. From the Site Users tab, select **New**.
3. On the ISA Entity Sites Users form, fill in the fields.
4. Select **Submit**.
The user is assigned to the site.

What to do next

[Assign users to assignment groups](#)

Assign users to assignment groups

Add users to assignment groups so they can see the vulnerability items for their assigned site.

Before you begin

To allow users to see the vulnerability items for the sites you've assigned them to, add users to the OT VR assignment group for the site.

When OT vulnerable items are created, visibility is limited to:

- Users with the VR Remediation Owner (sn_vul.remediation_owner) role
- Membership in the Operational Technology Vulnerability Response assignment group associated with the site that the OT device belongs to

Role required: admin

Procedure

1. Open the group that corresponds to the Operational Technology Vulnerability Response assignment group for the site.
2. From the Group Members tab, select **Edit**.
3. Add the users from the Collection list into the Group Members List.
4. Select **Save**.
Users are assigned to the group and can see the vulnerability items for the assigned site. For more information about admin tasks, such as adding users to groups, see [User administration](#).

What to do next

[Assign vulnerable items to groups](#).

Assign vulnerable items to groups

Configure OT Vulnerability assignment rules.

Before you begin

OT Vulnerable Items can be assigned to site level groups or groups based on classification, depending on your remediation strategy.

Role required: sn_vul.manage_assignment_rules or admin

About this task

When Vulnerable Items are imported, they are assigned to the appropriate group based on Vulnerability Assignment Rules. Operational Technology Vulnerability Response ships with one OT vulnerability assignment rule, **Operational Technology (OT) assignment rule**, which assigns OT vulnerable item records (VIT) to the corresponding OT VR assignment group based on its site. If it does not belong to any site, or if there's no group specified on the site, the rule assigns to the OT VR Default Assignment Group.

For more information about creating Vulnerability Response assignment rules, see [Create or edit Vulnerability Response assignment rules](#).

Procedure

1. From the Vulnerability Assignment Rules list, select **Operational Technology (OT) assignment rule**.
2. Configure it based on your remediation strategy:
 - If your remediation strategy is to assign all OT Vulnerable Items to the site, set the execution order of the OT VR Assignment rule to be less than all other rules.
 - If your strategy is to assign by class and then assign to sites for all other classes, set the execution order of the OT VR Assignment Rule to be greater than all class-based rules.
3. Once the execution order is updated, set the OT VR Assignment Rule Active state to **true**.

What to do next

[Configure OT remediation target rules](#).

Configure OT remediation task rules

For remediation tasks that are created in the Industrial Workspace, update existing remediation task rules to prevent imported vulnerable items from automatically adding OT devices.

Before you begin

Role required: sn_vul.manage_group_rules or admin

When vulnerable items are imported, they can be added to remediation tasks based on configured remediation task rules. If you use Vulnerability Response for both IT and OT networks, you must modify a configuration if you group Vulnerability Items for remediation differently between IT and OT networks. Operational Technology Vulnerability Response provides a sample Remediation Task Rule record that is loaded with demo data to demonstrate how to exclude OT network vulnerabilities from being grouped automatically.

Configure any new or existing Remediation Task Rules based on your remediation strategy:

- If your remediation strategy is to automatically create remediation tasks only for vulnerabilities within your IT environment, add the following condition to each existing remediation task rule to exclude OT vulnerabilities:
 - Configuration Item . OT device details = **is empty**
- If your remediation strategy is to automatically create remediation tasks for all OT vulnerable items, create an appropriate rule.

Sample shipped with OT VR demo data: Remediation Task Rule - Vulnerability (exclude OT)

A remediation task rule defines how a set of vulnerable items are automatically grouped for remediation. Define your rules such that all vulnerable items within a group are remediated by the same team, same remediation action, and same timeframe. For example, group by vulnerable item "Assignment group", "Vulnerability", and CI "Used for" (ex. Production, Staging, Development) if those environments have different maintenance windows. Vulnerable items that are not in the Open state are always excluded.

* Name: Vulnerability (exclude OT)

Description: NOTE - this rule is necessary to avoid including OT assets automatically into remediation tasks - every remediation task rule will need to add an "AND" clause to do this. This is a copy of the existing "Vulnerability" remediation task rule, just renamed with the additional condition "Configuration item . OT asset details = empty"

Case sensitive:

Condition: All of these conditions must be met

AND: Active Is true OR AND Configuration item . OT asset details Is empty OR AND

or New Criteria

Group by:

Choose the vulnerable item fields to group by. If an extended table field is chosen, the field will be used only for vulnerable items that use the extended table.

Group vulnerable items from: Vulnerable Item Using field: Assignment group

And then from: Vulnerable Item Using field: Vulnerability

And then from: Vulnerable Item Using field: Click to select...

Assignment:

If this rule groups vulnerable items by a user group field, such as vulnerable item "Assignment group", the remediation tasks can be assigned to match (Recommended). Use Assignment Rules to automatically set the vulnerable item "Assignment group" field for use in remediation task rules. Assign remediation tasks using the "Group by" field that specifies the desired user group field.

For example, a rule that groups on vulnerable item "Assignment group" could create separate groups for vulnerable items assigned to Windows Server, Database and Network. Each remediation task itself would then be assigned to Windows Server, Database and Network respectively.

Alternatively, remediation tasks created by this rule can be set to a static user group.

Assign remediation tasks by: Group by field: Assignment group

* Group by field: Assignment group

Procedure

1. Navigate to **Vulnerability Response > Administration > Remediation Task Rules**.

2. Select the name of the rule you want to update.

- Define the rules such that all vulnerable items within a group are remediated by the same team, the same remediation action, and the same timeframe. For example, group by vulnerable item "Assignment group", "Vulnerability", and CI "Used for" (ex. Production, Staging, Development) if those environments have different maintenance windows.
- For more information about remediation task rules, see [Vulnerability Response Workspaces](#). ↗
- For more information about remediation tasks, see [Explore the IT Remediation Workspace](#). ↗

Configure OT remediation target rules

Configure remediation target rules for OT vulnerable items.

To calculate the remediation target date for OT vulnerable items, load the demo data records for the Operational Technology Vulnerability Response application and configure the remediation target rules.

Role required: sn_vul.manage_remediation_target_rules or sn_vul.vulnerability_admin

OT Remediation Targets may be different due to the infrequent opportunities to perform maintenance in an industrial environment. Remediation target rules are applied in order from smallest target to largest target.

A different remediation target date may be needed for OT device vulnerabilities that do not have maintenance windows available in the same time frame as other vulnerabilities. To demonstrate how to configure remediation target dates in this situation, two demo data records are provided to demonstrate how this can be managed for Critical risk ratings:

- Critical Risk Rating rule (OT only) - This rule uses the condition of **Configuration item.OT device details is not empty AND Risk rating = 1 - Critical**. Update the Target (days) and activate the record.
- Critical Risk Rating rule (exclude OT) - In order to apply a shorter target to Critical Risk non-OT items only, you need to filter out OT devices first. This rule uses the condition **Configuration item.OT device details is empty AND Risk rating = 1 - Critical**. Update the Target (days), inactivate any existing critical target rule, and activate this rule in its place.

Note: Both of these rules must be activated so that any OT critical risk vulnerabilities are excluded from the non-OT remediation target rule.

For more information about creating Vulnerability Response assignment rules, see:

- [Vulnerability Response remediation target rules](#)
- [Create or edit Vulnerability Response remediation target rules](#)

Configure risk calculators

Configure risk calculators

Determine which OT risk factors to use when calculating the risk of a vulnerable item on an OT device.

Before you begin

In Operational Technology, additional factors can include the OT device criticality, the Purdue Level, and the criticality of the production process that the OT device automates.

Role required: sn_vul.manage_risk_score_configuration or admin

About this task

For this step, refer to the Default Risk Calculator with OT vulnerability calculator shipped with the Operational Technology Vulnerability Response application demo data. The Default Risk Calculator with OT is used when risk must be calculated differently for OT and non-OT vulnerable items.

Note: Because only one vulnerability calculator can be active at a time, the provided Default Risk Rule (non OT) is used as an example for calculating risk for all non-OT vulnerable items.

For more information, see [Define fields and weights for the risk rule](#).

To set the risk score for OT vulnerable items, adjust the weights for the risk rule records of the OT Default Risk Rule in the demo data. More fields available for OT in the demo data include:

- Equipment Model Entity Criticality - Use the Service Business criticality rule.
- OT Device Criticality - Use the Configuration item OT device details Device Criticality rule.
- Purdue Level - Use the Configuration item OT device details Purdue level field.

Procedure

1. Navigate to **Vulnerability Calculators**.
2. From the Vulnerability Calculators list, select **Default Risk Calculator with OT**.
3. From the Vulnerability Calculators Rules list, open the risk rule that you want to edit.
For example, select **OT Default Risk Rule**.

4. In the Risk Calculator Criteria section of the Vulnerability Risk Rule page, select a risk rule field.
5. On the Risk rule field record, update the weight or the weightage % for each criterion according to its importance in the overall risk score calculation.
6. Select **Update**.

What to do next

To set the risk score for all other vulnerable items, copy the existing risk rules to the Default Risk Calculator with OT, and set the order to run after the OT Default Risk Rule.

Configure OT vulnerability risk rollup calculator

Use the OT vulnerability risk rollup calculator to calculate the risk score of the OT devices at each level of the equipment model. The overall risk score is rolled up to the parent equipment model entity.

Before you begin

To calculate the risk score for all the equipment model entities, execute the scheduled job.

Note:

The risk score calculation for all the equipment model entities is only for the subsequent run of the daily schedule job.

Check that the service populator field in the list view of equipment model entities is set to OTDynamicManualServicePopulator. If it is set to other values, execute the on-demand job *Update ISA entity service populator*.

Role required: admin

About this task

For this step, refer to the Vulnerability Rollup Calculators with OT vulnerability calculator shipped with the Operational Technology Vulnerability Response application demo data.

For more information, see [Vulnerability Response Rollup Calculators](#).

To calculate the risk score for the equipment model entity, set up the weights for these fields:

- Maximum risk score of the Vulnerable Items (VITs) associated to the equipment model entity.
- Average risk score of the VITs associated to the equipment model entity.
- Number of vulnerable items per equipment model entity.

Procedure

1. Navigate to **All > Vulnerability Response > Administration > Vulnerability Rollup Calculator**.
2. From the Vulnerability Rollup Calculators list, select **Equipment Model Entity Rollup**.
3. If required, in the Rollup Weights section, update the weight for each criterion.
4. Select **Update**.

What to do next

To calculate the risk associated at a level for the equipment model entity, execute the scheduled job at a required time based on your business needs.

Note: the scheduled job as active to execute at a scheduled time. By default, the schedule is set to execute daily.

To calculate the risk rollup for all equipment model entities, navigate to **All > Industrial Workspace Admin > Guided Setup > Operational Technology Vulnerability Response > Risk roll up calculation > Risk rollup configuration score**.

To configure the scheduled job, navigate to **All > Industrial Workspace Admin > Guided Setup > Operational Technology Vulnerability Response > Risk roll up calculation > Daily Schedule job for risk roll up**.

The daily scheduled job runs every day without user intervention. If required, you can modify the execution time.

If necessary, all Equipment model entities can be considered for the risk score calculation for the next run of the daily schedule job.

To configure the Entities for Risk score rollup, navigate to **All > Industrial Workspace Admin > Guided Setup > Operational Technology Vulnerability Response > Risk roll up calculation > Entities for Risk score rollup**.

Install certified Vulnerability Response integrations

Integrate certified third-party applications that enhance functionality of OT vulnerability management.

Search the ServiceNow® Store for Operational Technology Certified integrations for the Operational Technology Vulnerability Response application, and install those applicable to your environment.

Operational Technology Vulnerability Response Integrations

The Operational Technology Vulnerability Response application includes support for third-party integrations.

The following third-party integrations are currently supported.

- Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)
- Vulnerability Response Integration with Claroty CTD.

Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)

The Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) uses data imported from Microsoft Defender for IoT (on-premises) to enable risk-based action with the production process context.

Use the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application to track, prioritize, and resolve vulnerabilities on devices used in the production process.

Key Features

- Import CVEs associated with OT devices from Microsoft Defender for IoT (On-Premises Management Console) and create vulnerable items (VITs) to provide a single view of OT devices vulnerability data with production process context.
- Run imports of newly detected vulnerabilities automatically on your own schedule.
- Using assignment rules for VITs can be automatically routed for remediation to local site-based teams to take risk-based action.

Install the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)

You can install the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) if you have the admin role. The application includes installs related ServiceNow® Store applications and plugins if they are not already installed.

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](#).
- Review the [Vulnerability Response for Microsoft Defender for IoT \(On-premises Management Console\)](#) application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.
- Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) requires the following ServiceNow Store applications. Ensure that these applications are installed before you install the Vulnerability Response integration with Microsoft Defender for IoT.

CMDB CI Class Models store app

This integration uses the Operational Technology [extension classes](#) that are part of the CMDB CI Class Models application. For more information, see [CMDB CI Class Models store app](#).

Service Graph Connector Microsoft Defender for IoT (on-premises)

This integration uses the Operational Technology Manager application to automate the import of sensor appliances, OT devices, and network connections. To install the Service Graph, see [Service Graph Connector for Microsoft Defender for IoT \(On-premises Management Console\)](#).

Role required: admin

About this task

The following items are installed with Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console):

- Vulnerability response plugin
- Vulnerability Response Integration with NVD

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) using the filter criteria and search bar.

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

In the list next to the **Install** button, the versions that are available to you are displayed.

3. Select a version from the list and select **Install**.

In the Install dialog box that is displayed, any dependencies that are installed along with your application are listed.

4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.

5. Select **Install**.

Assign Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following tables can use the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application.

Assign roles to admin users or user groups as needed.

Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) roles

Role	Description
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view OT VR integration records.
OT VR Integration Admin [sn_otvr.integration_admin]	Can configure and execute OT VR integration.
MID server [mid_server]	Can configure MID Server.

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Run the National Vulnerability Database integration

Run the National Vulnerability Database (NVD) integration to import data from the National Institute of Standards and Technology (NIST) NVD product. Running the NVD integration helps

you determine the severity and details of Common Vulnerabilities and Exposures (CVEs) found in your environment.

Before you begin

Before you run the NIST NVD integration on your instance, the installation and configuration steps must be completed. Completing the installation and configuration ensures that the NVD product properly integrates with the Operational Technology Vulnerability Response application.

To install the NVD plugin, see [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#).

Role required: admin

Procedure

1. Navigate to All > Vulnerability Response > Administration > Integrations.

2. Select the NIST NVD integration - API (CVE only) record.

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response I...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response I...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response I...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. In the Import Since field, set the value to NULL.

4. Select Execute Now.

Configure the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)

Configure the record for the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) integration.

Before you begin

Use the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) guided setup to complete the configuration. To access the Guided Setup, navigate to **MSFT D4IoT Vulnerability Integration > Administration > Guided Setup**.

Role required: sn_otvr.integration_admin and mid_server

Procedure

1. Navigate to All > MSFT D4IoT Vulnerability Integration > Administration > Configurations.

2. Click New.

3. On the form, fill in the fields.

For a description of the field values, see [Microsoft Defender for IoT VR Configuration form](#).

4. Click Save and Verify Credentials.

Microsoft Defender for IoT VR Configuration form

Use the Microsoft Defender for IoT VR Configuration form to configure the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application.

Microsoft Defender for IoT VR Configuration form

Field	Description
Name	The name of the configuration.
Integration instance	<p>The instance for the configuration.</p> <p>The available default integration instance is the Microsoft Defender for IoT Vulnerability Response instance.</p>
Endpoint URL	<p>The URL of the Microsoft Defender for IoT Management Console.</p> <p>For example: https://10.10.0.222/external/v3/integration/devicecvcs</p>
MID server	The MID Server used for the integration.
API key	<p>The token needed to access the Central Manager APIs.</p> <p>For information about creating an API key in the Microsoft Defender for IoT management console, see https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis.</p>
Page size	<p>The number of devices per page in the Microsoft API response.</p> <p>The default page size is 50.</p>
CVSS V2 Score	<p>The vulnerabilities with the score greater than or equal to the configured CVSS V2 score is considered for the import of CVEs and creation of Vulnerable Item (VI) records.</p> <p>The default value is set to 0.</p>
Auto-close Resolved VIs	If the Vulnerable Item record is set to resolved, it can be closed automatically if the CVE no longer appears in the API response from Microsoft Defender for IoT for that OT device.
Wait days to reopen a Resolved VI	<p>When a VI is resolved, it can take a while for Microsoft Defender for IoT to confirm if the vulnerability is resolved based on the OT device's communication in the network.</p> <p>Define the number of days to wait before reopening the resolved VI when the NIDS cannot confirm it as Closed.</p>

Configure import schedules

Configure the import schedules to access the Microsoft Defender for IoT records.

Before you begin

Before scheduling the import of Microsoft Defender for IoT records, run the NVD integration to fix any issue. For more information, see [Run the National Vulnerability Database integration](#).

Role required: admin

Procedure

1. Navigate to **All > MSFT D4IoT Vulnerability Integration > Administration > Integrations**.
 2. From the list of records, select your record:
 - The **Full Import** schedule imports all the vulnerabilities for all OT devices.
- i Note:** Frequent execution of the Full Import Schedule is not recommended because the number of records can be high.
- The **Delta Import** schedule can be configured by default to run after the Microsoft Service Graph Connections integration. See [Configure the system ID of the OT Vulnerability Response integration](#).
 - Use the **Auto-close Resolved VIT Import** schedule if the vulnerability on the OT device is resolved. The Vulnerable Items (VITs) are closed automatically based on the confirmation from the scanner.

If the scope is not in the correct application, the message To edit this record click here appears on the top of the page.

3. Click **here** to edit the record.
4. Select the **Active** check box to change **Active** to **true**.
5. Select **Schedule** from the drop-down list as required.
6. Click **Execute Now**.

Configure the system ID of the OT Vulnerability Response integration

Configure the system ID to import integration records fully after the Microsoft SGC Connections integration.

Before you begin

Role required: admin

About this task

This configuration is strongly recommended to ensure all OT devices are in the CMDB that may have vulnerabilities reported against them.

Procedure

1. Navigate to **All > Service Graph Connector Microsoft D4 IoT > Properties**.

If the scope is set to the wrong application, the message To edit this record click here appears at the top of the page.

This record is in the [Service Graph Connector Integration with Microsoft Azure Defender for IoT application](#), but [Global](#) is the current application. To edit this record click [here](#).

Microsoft Defender for IoT Integration Properties

Integration Configurations

The following system properties are used to configure the Microsoft Defender for IoT integration.

Sensor API resource path. Default value is "/external/v3/integration/sensors". [?](#)

Device API resource path. Default value is "/external/v3/integration/devices". [?](#)

Connection API resource path. Default value is "/external/v3/integration/connections". [?](#)

(Optional) Override Connection Alias record sys_id used to connect the integration. Default value is empty. [?](#)

The number of device records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. [?](#)

The number of connection records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. [?](#)

Get all devices. If not checked, then only devices created or updated since the last successful import will be imported. Default is No. [?](#)
 Yes | No

Get all connections. If not checked, then only connections created or updated since the last successful import will be imported. Default is No. [?](#)
 Yes | No

(Optional) Sys id of OT VR Integration (Scheduled Job) to execute after SG-OT Microsoft D4IoT Connections Import. [?](#)

Save

2. Click **here** to edit the record.
3. Configure the system property `sn_msftd4iotsgc.ot.vr.integration.id` with the `sys_id` of the OT VR Integration.
4. Click **Save**.

Configure Auto-Close Stale Detections

The Auto-Close Stale Vulnerable Items setting helps you clean up older, stale vulnerable items (VITs) not recently found by your third-party integrations.

Before you begin

Role required: admin

About this task

These stale detections most likely result from a remediation targeted for a critical risk VIT also addressing multiple additional lower criticality VITs that may still be in the "open" state. Moving these VITs to **Closed** reduces the number of active vulnerable items and vulnerability groups in your Now Platform instance.

Procedure

1. Navigate to **All > Vulnerability Response > Administration > Auto-Close Configuration**.
The Auto-Close Configuration form is displayed.
2. For the **Auto-close stale items based on** field, select **Detections last found** in the list.

Note:

The **Devices last scanned** is not applicable for OT scanners.

3. To enable the module, select the **Active** check box to select it.
4. In the **days ago** field, enter the age of older, stale VITs in the number of days that you want to close.

The default is 90 days. You can enter any positive value for the number of days. This value is used to match a last detected date provided by Microsoft Defender for IoT. With 90 and **Vulnerable items last detected** displayed, any vulnerable items not detected in the last 90 days are automatically closed.

5. Select **Update**.

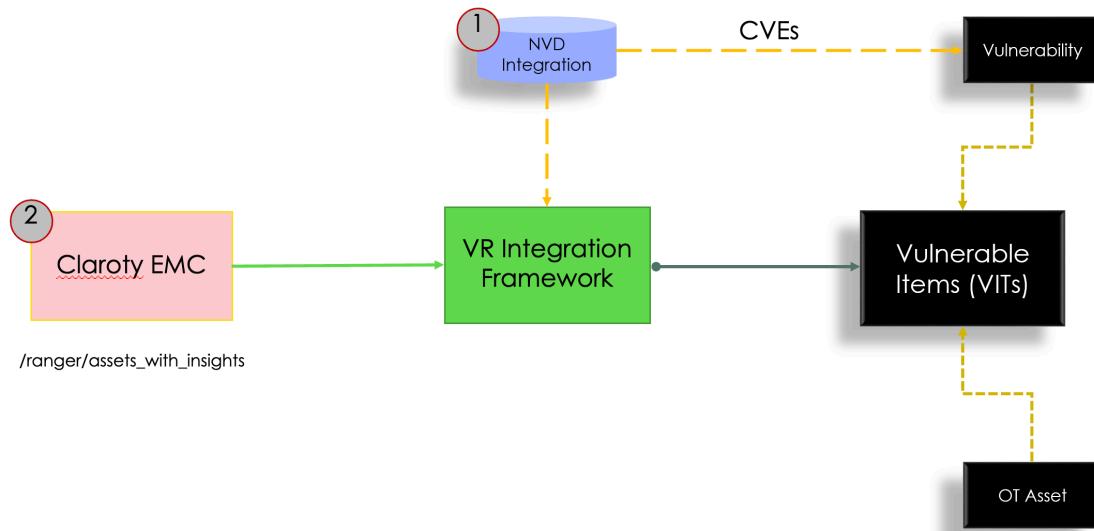
Vulnerability Response Integration with Claroty CTD

The Vulnerability Response Integration with Claroty Continuous Threat Detection (CTD) uses vulnerability data imported from Claroty CTD to enable risk-based action within the production process.

Use this Vulnerability Response Integration with the ServiceNow® Operational Technology Vulnerability Response application to track, prioritize, and resolve vulnerabilities used in the production process.

The following image shows the process for the Vulnerability Response Integration with Claroty CTD.

Process for the Vulnerability Response Integration with Claroty CTD



Before you run the Vulnerability Response Integration with Claroty CTD, you must run the National Vulnerability Database (NVD) integration. The NVD integration fetches published Common Vulnerabilities and Exposures (CVEs) from the NVD and populates them in ServiceNow. Then when you run the Vulnerability Response Integration with Claroty CTD application, the application identifies the vulnerabilities for each device and creates vulnerable items (VIs).

Each VI has a relationship with an Operational Technology (OT) device, or Configuration Item (CI), and the vulnerability that's detected. The vulnerability integration framework

establishes a connection with the Claroty Enterprise Management Console (EMC) and pulls the vulnerabilities for all OT devices.

Key features

- Import common vulnerabilities and exposures (CVEs) associated with Operational Technology (OT) devices from Claroty CTD. Create vulnerable items (VITs) to provide a single view of OT device vulnerability data and how it affects the production process.
- Run imports of newly detected vulnerabilities automatically on your own schedule.
- Use assignment rules to route VITs automatically for remediation to local site-based teams that can take risk-based actions.

Install Vulnerability Response Integration with Claroty CTD

Install the Vulnerability Response Integration with Claroty CTD (sn_clarotyctdvr). The application includes installs related ServiceNow® Store applications and plugins if they aren't already installed.

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](#).
- Review the [Vulnerability Response Integration with Claroty CTD](#) application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.
- Vulnerability Response Integration with Claroty CTD requires the following ServiceNow Store applications. Ensure that these applications are installed before you install the Vulnerability Response Integration with Claroty CTD.

CMDB CI Class Models store app

This integration uses the Operational Technology [extension classes](#) that are part of the CMDB CI Class Models application. For more information, see [CMDB CI Class Models store app](#).

Service Graph Connector Integration for Claroty CTD

This integration uses the Operational Technology Manager application to automate the import of sites, detected devices by each site, connections (or base systems), and installed programs to the Configuration Management Database (CMDB). To install the Service Graph Connector Integration for Claroty CTD, see [Install Vulnerability Response Integration with Claroty CTD](#).

Role required: admin

About this task

The following items are installed with Vulnerability Response Integration with Claroty CTD:

- Vulnerability response plugin
- Vulnerability Response Integration with NVD

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Vulnerability Response Integration with Claroty CTD application (sn_clarotyctdvr) 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 might have to request it from the ServiceNow Store.

In the list next to the **Install** button, the versions that are available to you are displayed.

3. Select a version from the list and select **Install**.

In the Install dialog box that is displayed, any dependencies that are installed along with your application are listed.

4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.

5. Select **Install**.

Assign Vulnerability Response Integration with Claroty CTD roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Vulnerability Response Integration with the Claroty CTD application.

Before you begin

Role required: admin

About this task

When you're assigned the roles listed in the following table, you can use the Vulnerability Response Integration with Claroty CTD application.

Assign roles to admin users or user groups as needed.

For more information about the roles available for the Vulnerability Response Integration with Claroty CTD application, see [Vulnerability Response Integration with Claroty CTD roles](#).

Procedure

Assign roles to users or groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Vulnerability Response Integration with Claroty CTD roles

Roles control access to features and capabilities in the Vulnerability Response Integration with Claroty CTD.

The following table describes the roles and permissions for the Vulnerability Response Integration with Claroty CTD.

Vulnerability Response Integration with Claroty CTD roles

Role	Description
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view OT VR integration records.
OT VR Integration Admin [sn_otvr.integration_admin]	Can configure and execute the OT VR integration.

Vulnerability Response Integration with Claroty CTD roles (continued)

Role	Description
MID server [mid_server]	Can configure a MID Server.

Run the National Vulnerability Database integration

Run the National Vulnerability Database (NVD) integration to import data from the National Institute of Standards and Technology (NIST) NVD product. Running the NVD integration helps you determine the severity and details of Common Vulnerabilities and Exposures (CVEs) found in your environment.

Before you begin

Before you run the NIST NVD integration on your instance, the installation and configuration steps must be completed. Completing the installation and configuration ensures that the NVD product properly integrates with the Operational Technology Vulnerability Response application.

To install the NVD plugin, see [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#).

Role required: admin

Procedure

1. Navigate to All > Vulnerability Response > Administration > Integrations.
2. Select the NIST NVD integration - API (CVE only) record.

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response ...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response ...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response ...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. In the **Import Since** field, set the value to **NULL**.

4. Select **Execute Now**.

Configure the Vulnerability Response Integration with Claroty CTD

Configure the Vulnerability Response Integration with Claroty CTD to begin importing data.

Use the Claroty CTD Vulnerability Integration Guided Setup to complete the configuration.

To access the Claroty CTD Vulnerability Integration Guided Setup, navigate to **Claroty CTD Vulnerability Integration > Admin > Setup**.

Connect to the Claroty CTD

Connect to the Claroty CTD to begin the Vulnerability Integration setup.

Before you begin

Before performing the setup, change the application scope to **Vulnerability Response**

Integration with Claroty CTD by selecting the globe icon () in the navigation bar.

Role required: admin

Procedure

1. Navigate to **All > Claroty CTD Vulnerability Integration > Admin > Setup**.
2. In the Connect to Claroty CTD section, select the **Setup Connections** task.
3. On the Setup Connections task page, select **Configure**.
The Claroty CTD Connection Manager page opens.
4. On the form, fill in the following fields.

Connect to Claroty CTD form

Field	Description
Claroty EMC URL	URL of the Claroty CTD Enterprise Management Console (EMC).
Minimum CVSS Score	If applicable, you can filter which vulnerabilities are imported based on their Common Vulnerability Scoring System (CVSS) score. This is a greater than or equal filter, so if you enter "9.0" the integration imports vulnerabilities with a CVSS score of 9.0-10.0.
User Name	Claroty account user name.
Password	Claroty account password.
MID Server	If your Claroty EMC is on-premises, a MID Server may be required. If so, select a MID Server here.

5. Select **Update**.

6. Select **Test Connection**.

If the connection test is successful, a **Results 200** output message appears. An unsuccessful connection attempt displays the error code and the message received from Claroty.

Activate the Delta Import integration

Activate the Delta Import integration to import vulnerabilities from Claroty CTD.

Before you begin

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see [Run the National Vulnerability Database integration](#).

Role required: admin

About this task

The Delta Import integration imports vulnerabilities from Claroty CTD from the last successful integration run. By default, the first run imports the past 90 days of data. Clearing the **Start time** field results in a full import.

Procedure

1. Navigate to **All > Claroty CTD Vulnerability Integration > Admin > Setup**.
2. In the Configure Integration Scheduled Jobs section, select the **Activate Delta Import Integration** task.
3. Select **Configure**.
4. Ensure the Delta Import integration record is set to **Active**.
5. Ensure that the **Run** field is set to **On Demand**.
6. Optional: To execute a full import, clear the **Start time** field.
7. Select **Update**.

Run the Vulnerability Integration after the Service Graph Connector

Run the Claroty CTD Vulnerability Integration after running the Service Graph Connector for Claroty CTD. Running the Vulnerability Integration immediately after running the Service Graph Connector ensures that the most up to date CMDB information is populated from Claroty CTD.

Before you begin

The Service Graph Connector Integration for Claroty CTD must be configured and active in order to run the Vulnerability Response Integration to run after the Service Graph Connector.

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see [Run the National Vulnerability Database integration](#).

Role required: admin

Procedure

1. Navigate to **All > Claroty CTD Vulnerability Integration > Admin > Setup**.
2. In the Configure Integration Scheduled Jobs task, select the **Run After Service Graph Connector** tab.
3. Select **Configure**.
4. For the Run After SGC - Claroty CTD Vulnerability Detection Integration - Delta Import record, activate it by selecting the **Active** option.
5. Ensure the **Run** field is set to **After Parent Runs**.
6. Ensure the **Parent** field is set to **SG-OT Claroty CTD Assets Scheduled Import**.
7. Select **Update**.

Activate the Auto-Closure Integration

Activate the auto-closure integration to close the corresponding ServiceNow Vulnerability Detections.

Before you begin

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see [Run the National Vulnerability Database integration](#).

Role required: admin

About this task

There are two closure integration jobs available for the Vulnerability Response Integration with Claroty CTD:

- Claroty CTD Resolved Vulnerability Closure Integration
- Claroty CTD Full Vulnerability Closure Integration

The Claroty CTD Resolved Vulnerability Closure Integration checks for the vulnerable items (VITs) that have been marked as **Resolved** in the ServiceNow Configuration Management Database (CMDB). It then queries Claroty CTD for these VITs and closes them based on the response obtained from Claroty CTD.

The Claroty CTD Full Vulnerability Closure Integration checks for all VITs regardless of their state (Resolved or not) in the ServiceNow CMDB. It then queries Claroty CTD for all the VITs, and closes those that don't have a corresponding CVE entry in Claroty CTD.

Procedure

1. Navigate to **All > Claroty CTD Vulnerability Integration > Admin > Setup**.
2. In the Configure Integration Scheduled Jobs task, select the **Activate Auto-Closure Integration** tab.
3. Select **Configure**.

i Note: The auto-closure integration is pre-configured to run after the Delta Import, so no scheduling is required.

4. Ensure that the **Run** field is set to **On Demand**.
5. Ensure that the record is set to **Active**.
6. Select **Update**.

Configure the Full Import Integration from Claroty CTD

Configure the Full Import Integration to import the entire vulnerability inventory of a device from Claroty CTD.

Before you begin

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see [Run the National Vulnerability Database integration](#).

Role required: admin

About this task

The Claroty CTD Vulnerability Detections - Full Import integration imports the entire vulnerability inventory of a device from Claroty CTD without respect to a certain date. This integration is useful if the daily delta imports haven't imported all the necessary vulnerability data.

i Note: The Full Import integration respects the Minimum CVSS Score configuration. If you configured the integration to import only CVSS 9.0 and above, the Full Import only imports CVSS 9.0 and above.

Procedure

1. Navigate to **All > Claroty CTD Vulnerability Integration > Admin > Setup**.
2. In the Configure Integration Scheduled Jobs task, select the **Configure Full Import Integration** tab.
3. Select **Configure**.
4. Ensure that the **Run** field is set to **On Demand**.

5. Ensure that the record is set to **Active**.

6. Select **Update**.

Set the system properties

Set the system properties for the Vulnerability Response Integration with Claroty CTD so that you can enable the properties as needed.

Before you begin

Before performing the setup, change the application scope to **Vulnerability Response Integration with Claroty CTD** by selecting the Globe icon () in the navigation bar.

Role required: sn_otvr.integration_admin

Procedure

1. Navigate to **All > Claroty CTD Vulnerability Integration > Admin > Properties**

2. Update the system property records as needed for your organization.

For more information about the system properties installed for the Vulnerability Response Integration with Claroty CTD application, see [Properties installed for the Vulnerability Response Integration with Claroty CTD](#).

3. Select **Update** and save your changes.

Properties installed for the Vulnerability Response Integration with Claroty CTD

You can enable system properties for the Vulnerability Response Integration with Claroty CTD application.

To access the Vulnerability Response Integration with Claroty CTD system properties, navigate to **All > Claroty CTD Vulnerability Integration > Admin > Properties**.

System properties

Name	Description	Type	Default value
sn_clarotyctdvr.api_token_lifespan	The length of time the Claroty CTD API token is valid. Default is 480 minutes (8 hours).	integer	480
sn_clarotyctdvr.api_token_subject	An OAuth subject that identifies access to the API.	string	{"customer_name": "", "first_name": "ServiceNow", "last_name": "API", "id": 1, "mail": null, "password": null}
sn_clarotyctdvr.auto_close_detections	Auto-close detections Vulnerability Detections from Claroty CTD.	true, false	false
sn_clarotyctdvr.auto_close_detections_after_days	Detection of detections after days Claroty CTD will be auto-closed after a designated number of days since Last Found.	integer	90

System properties (continued)

Name	Description	Type	Default value
sn_clarotyctdvr.default_number_of_records	The number of records to pull per page from the Claroty CTD API.	integer	500
sn_clarotyctdvr.detection_start_time_offset	When importing data, a buffer from the Claroty CTD API, a buffer of a designated number of hours is added before the "start time." This ensures that no records are missed in the Delta import.	integer	4
sn_clarotyctdvr.integration_default_days	By default, the first run of the integration imports data from a past number of days.	integer	90
sn_clarotyctdvr.require_ci	Requires incoming CI to match the CMDB to create Vulnerability Detections.	true, false	true

Data mapping for the Vulnerability Response Integration with Claroty CTD

This section specifies how fields from the Claroty CTD API are mapped to fields in the ServiceNow tables.

Vulnerability detection data mapping

Claroty CTD field	ServiceNow field	Notes
	Source	Always set to Claroty CTD .
Identified_on	First Found	
Last_updated	Last Found	
Status	Status	A status of 0 means Open . A status of 2 means Closed/Fixed .
Resource_id	Configuration item	The configuration item (CI) is set through a CI lookup rule that searches the sys_object_source table for the Resource ID. For example, 33.1.

Vulnerability entry data mapping

Vulnerability entries are only created if an existing Common Vulnerabilities and Exposures (CVE) record is not found in the National Vulnerability Database Entry [sn_vul_nvd_entry] table. If the Claroty CTD Integration must create a CVE, it maps the following source fields listed in the table.

Claroty CTD field	ServiceNow field	Notes
Cve_id	ID	Example: CVW-2017-17562
Title	Summary	The integration adds [Claroty] to the Summary so that the NVD CVEs, backfilled by Claroty, are visible. For example, the [Claroty] Authentication Bypass Vulnerability in SIPROTEC.
Cvss	V3_base_score	
Published	Date_published	
Modified	Last_modified	

Possible errors for the Vulnerability Response Integration with Claroty CTD

You may encounter errors that need troubleshooting while you're working with the Vulnerability Response Integration with Claroty CTD.

Vulnerability Detection Integration (Data Retrieval)

Error message	Possible cause
Can't run a Claroty CTD Integration without a user name and password combo.	No user name or password is present on the integration configuration.
Can't run integration without a REST message and REST method specified.	On the Claroty CTD Integration job record, the REST message or REST method fields aren't populated.
Can't run integration without Claroty CTD server URL specified.	No URL is present on the integration configuration.
Can't run integration without the detection API resource path specified.	On the integration configuration, the detection_api_resource_path parameter isn't populated. The default is /ranger/assets_with_insights.
Invalid response code {response code} received from Claroty CTD.	The response from the Claroty API was invalid. For example, the message Invalid response code 401 is received from Claroty CTD. This invalid response code means Unauthorized and that the credentials (user name/password) are likely invalid.
Unable to read the count_total property from JSON data.	The count_total used for pagination wasn't present in the API response. It likely means

Error message	Possible cause
	<p>that an invalid payload was received from Claroty CTD.</p> <p>Ensure that the Claroty CTD instance is reachable through the MID Server and examine the Data Source attachment <code>response.json</code> file to ensure that <code>count_total</code> exists.</p>

Vulnerability Detection Integration (Data Processing)

Error message	Possible cause
Error writing attachment.	<p>The system couldn't attach the response data to the Data Source. Contact your administrator for further assistance.</p> <p>A common cause for this error is that the MID Server user is missing the <code>sn_vul.vr_import_admin</code> role.</p>
Attachment content is null: attachment <code>sys_id = {sys_id}</code> .	The Data Source attachment content is null. This could indicate an issue with the Claroty API itself, or an issue in ServiceNow. Contact your administrator for further assistance.
Couldn't find attachment with <code>sys_id {sys_id}</code> .	Data Source attachment wasn't found. Follow the same procedures for the preceding error.

Vulnerability Auto-Closure Integration (Data Retrieval)

Error message	Possible cause
Can't run a Claroty CTD Integration without a user name and password combo.	No user name or password is present on the integration configuration.
Can't run integration without a REST message and REST method specified.	On the Claroty CTD Integration job record, the REST message or REST method fields aren't populated.
Can't run integration without Claroty CTD server URL specified.	No URL is present on the integration configuration.
Can't run integration without the detection API resource path specified.	On the integration configuration, the <code>detection_api_resource_path</code> parameter isn't populated. The default is <code>/ranger/assets_with_insights</code> .
Invalid response code {response code} received from Claroty CTD.	The response from the Claroty API was invalid. For example, the message <code>Invalid response code 401</code> is received from Claroty CTD. This invalid response code means Unauthorized and that the

Error message	Possible cause
	credentials (user name/password) are likely invalid.
Unable to read the count_total property from JSON data.	<p>The count_total used for pagination wasn't present in the API response. It likely means that an invalid payload was received from Claroty CTD.</p> <p>Ensure that the Claroty CTD instance is reachable through the MID Server and examine the Data Source attachment response.json file to ensure that count_total exists.</p>
Error parsing 'objects' array from response body.	Likely means that an invalid payload was received from Claroty CTD. Ensure that the Claroty CTD instance is reachable and check Outbound HTTP Logs to see if there was a valid response.

Vulnerability Auto-Closure Integration (Data Processing)

Error message	Possible cause
Failed to parse the Data Dictionary JSON.	The payload from the Data Source attachment was invalid JSON. Likely another error occurs before this error occurs. Ensure that the Claroty CTD instance is reachable and check Outbound HTTP Logs to see if there was a valid response.

Using Operational Technology Vulnerability Response

After you complete all required set up tasks, including importing vulnerable items from a third-party integration, you can use the Operational Technology Vulnerability Response application from the Industrial Workspace.

Industrial Workspace

To use Operational Technology Vulnerability Response, access the following landing page and menus from the Industrial Workspace.

For more information on the Industrial Workspace, see [Operational Technology Devices landing page tab](#).

OT Vulnerabilities landing page tab

Use the OT Vulnerabilities landing page tab in the Industrial Workspace landing page to view the following data:

- Summary of new OT vulnerable items created in the last 7 days.
- Summary of OT vulnerable items by risk score and by state.

- Any vulnerable items that are unaddressed (OT vulnerable items that have not yet been assigned and are in an open state).
- Summary of risk score of the OT devices at each level of the equipment model and list of the vulnerable items.

For more information about the OT Vulnerabilities landing page tab, see [Operational Technology Vulnerabilities landing page tab](#).

List menu

Use the List menu to view all OT Vulnerable Item records that you have access to and remediation tasks that have either been assigned to you or to an assignment group that you are a member of.

- OT Remediation Tasks
 - Assigned to me
 - Assigned to my groups
- OT Vulnerable Items
 - Assigned to me
 - Assigned to my groups
 - My Exception Requests
 - All Exceptions

i Note: The All Exceptions list also shows exceptions with a **Rejected** state.

Navigate to records under the OT Remediation Tasks or OT Vulnerable Items list menus to get more OT-related context. To view the history of the record, you can view the **Activity** window in the record where various work notes, comments, and record updates are captured. You can also add new comments or work notes in the **Compose** window.

For more information about remediation tasks, see [Create a remediation task](#).

For more information on how to use the List view in the Industrial Workspace for Operational Technology Vulnerability Response, see [Use the List view in the IT Remediation Workspace](#).

Equipment model menu

Use the Equipment Manager to view OT vulnerable items, and view and create remediation tasks associated with OT devices that are mapped to an equipment model entity.

Related topics

[Reviewing the Operational Technology Manager Workspace](#)

[Vulnerability Response Workspaces](#)

Create a remediation task

Create remediation tasks associated with OT devices that are mapped to an equipment model entity.

Before you begin

Role required: sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin

Procedure

1. Navigate to **All > Industrial Workspace**.
2. Open the **Equipment model** page.
3. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
4. Select the appropriate equipment model entity and navigate to the **Vulnerable Items** related list tab.
5. Select the vulnerable item records you want to add to the remediation task, then select **Create remediation task**.

The screenshot shows the ServiceNow interface for the Industrial Workspace. The top navigation bar includes 'servicenow', 'All', 'Favorites', 'History', 'Workspaces', 'Admin', and a search bar. The main title is 'Equipment model view for San Diego'. On the left, a sidebar shows a tree structure with 'San Diego' expanded, showing 'Airport' and 'Terminal 1' (which is selected). The main content area displays a table titled 'Vulnerable Items [41]'. The table columns are: Number, Summary, OT asset, Manufacturer, Risk score, Risk rating, State, and Remediation tasks. There are 20 rows visible, each representing a different vulnerability record. The first two rows are highlighted in blue, indicating they are selected. The 'Summary' column contains brief descriptions of the vulnerabilities, such as 'Clarity! Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration'. The 'Risk rating' column uses color-coded icons: green for '5 - None', orange for '2 - High', and purple for '3 - Medium'. The 'State' column shows 'Open' for all items. At the bottom of the table, there are pagination controls (Showing 1-20 of 41) and a 'rows per page' dropdown set to 20.

6. Provide all the required details for the remediation task.
The Assignment group field automatically assigns based on the site assignment group.
7. Select **Save** to create the task record.

What to do next

Select a start time for the remediation task. For more information, see [Select a start time for a remediation task](#).

Select a start time for a remediation task

Select an expected start time for an Operational Technology (OT) remediation task by using the time slots in the equipment model entity schedules.

Before you begin

Role required: sn_vul.remediation_owner

About this task

There are two ways to select a start time for an OT remediation task.

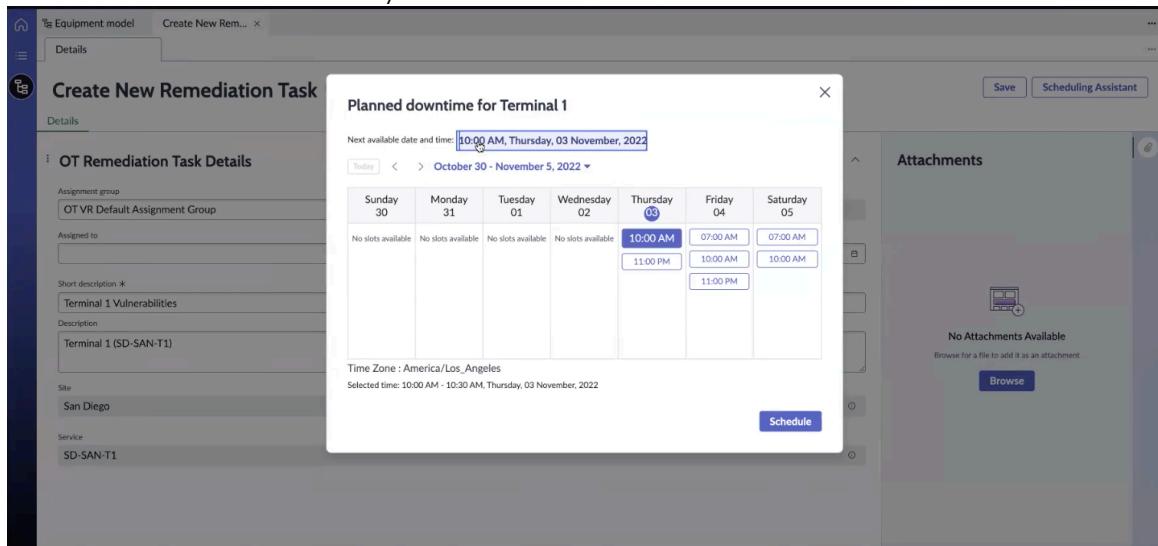
- You can select a start time when creating a remediation task by selecting **Scheduling Assistant** on the Create New Remediation Task form.
- You can open an existing remediation task and schedule from there.

The Scheduling Assistant uses the time slots from the equipment model entity schedules. For more information, see [Managing an equipment model entity schedule](#).

Procedure

- If you want to select a start time while creating a remediation task, do these actions:

- Refer to [Create a remediation task](#) and complete steps 1-6.
- Select **Scheduling Assistant**.
- Select the date and time slot when you'd like the remediation task to take



place.

- Select **Schedule**.

- If you want to select a start time for an existing remediation task, do these actions:

- Navigate to **All > Industrial Workspace**.
- In the list view, navigate to **OT Remediation Tasks > Assigned to me**.
- From the list, select the remediation task that you want to set a start time for.
- Select **Scheduling Assistant**.
- Select the date and time slot when you'd like the remediation task to take place.
- Select **Schedule**.

Result

The remediation task takes place during the set time.

Split remediation task

User can split the Vulnerable items (VIs) from a remediation task record to create a remediation task.

Before you begin

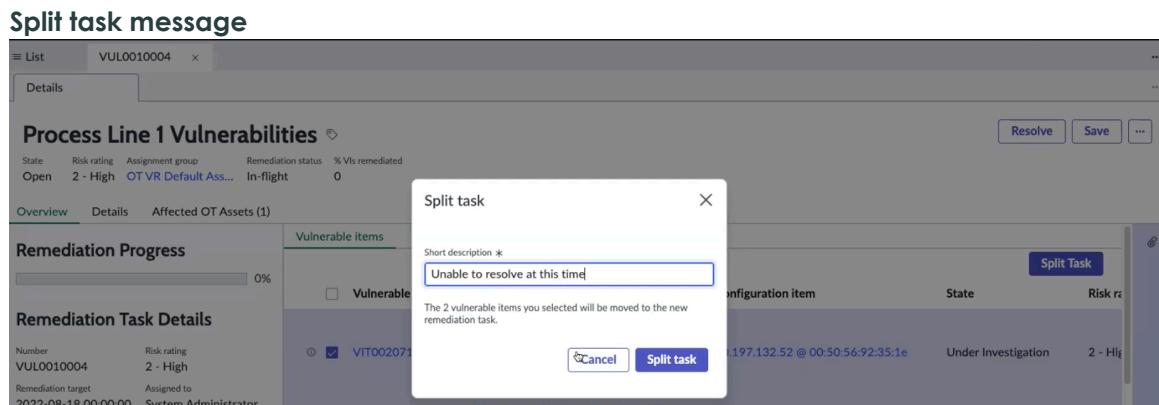
Role required: admin

Procedure

- Navigate to **All > Industrial Workspace > OT Remediation Tasks > Assigned to Me**.
- From the list, select the VIs that you want to move to a new remediation task.
- Click **Split Task**.

4. In the dialog that is displayed, fill the short description field.

The number of VIs you selected from the list is displayed.



5. Click **Split Task** again.

Operational Technology Vulnerability Response reference

Reference topics provide additional information about the Operational Technology Vulnerability Response application. At time of publication, this section contains no topics.

Related information

For more information about the Operational Technology (OT) product view related to the Common Service Data Model (CSDM), the Network Intrusion Detection System (NIDS), OT extension classes, and related applications see the following.

Overview

The product view and the extension classes help you understand how Operational Technology Management works with the CSDM framework and the Configuration Management Database (CMDB) respectively.

[Operational Technology product view](#)

The Operational Technology product view helps you understand how Operational Technology key entities work with the CSDM framework.

[Network Intrusion Detection System \(NIDS\) CI extension class](#)

The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.

[Operational Technology \(OT\) extension classes](#)

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

[Vulnerability Response](#)

When integrated with Operational Technology Vulnerability Response, the ServiceNow Vulnerability Response application aids you in prioritizing and resolving OT vulnerabilities based on process criticality.

[CMDB CI Class Models store app](#)

The CMDB CI Class Models store app adds class models that extend the CMDB class hierarchy, including class descriptions, identification rules, identifier entries, and dependent relationships.

Industrial Process Manager

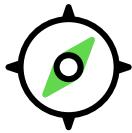
Use the Industrial Process Manager application to create the ISA-95 Equipment Model data foundation that is required for the ServiceNow Industrial solution, enabling you to create your own version of the equipment models in each of your industrial sites.

Operational Technology Manager

The Operational Technology Manager application enables you to aggregate OT device data from multiple sources, so that you can build the foundational data relationships used in the Industrial solution.

Operational Technology Incident Management

Operational Technology Incident Management enables manufacturers to manage OT device incidents from open to closure.

<p>Explore</p>  <p>Exploring Operational Technology Incident Management</p>	<p>Configure</p>  <p>Plan and configure your implementation</p>
<p>Use</p>  <p>Using Operational Technology Incident Management</p>	<p>Reference</p>  <p>Get details about related information and applications</p>

Exploring Operational Technology Incident Management

Learn more about the Operational Technology Incident Management application.

Key features

With Operational Technology Incident Management, you can use the following key features.

- Create OT incidents and drive workflows to quickly restore production processes impacted by OT devices.
- Understand context and impact of OT incidents on production processes.

- Monitor and manage OT incidents separately from IT incidents.
- Assign a separate role for the OT incident fulfiller.
- Improved OT user experience.
- Support for Operational Technology Knowledge Management. For more information, see [Operational Technology Knowledge Management](#).

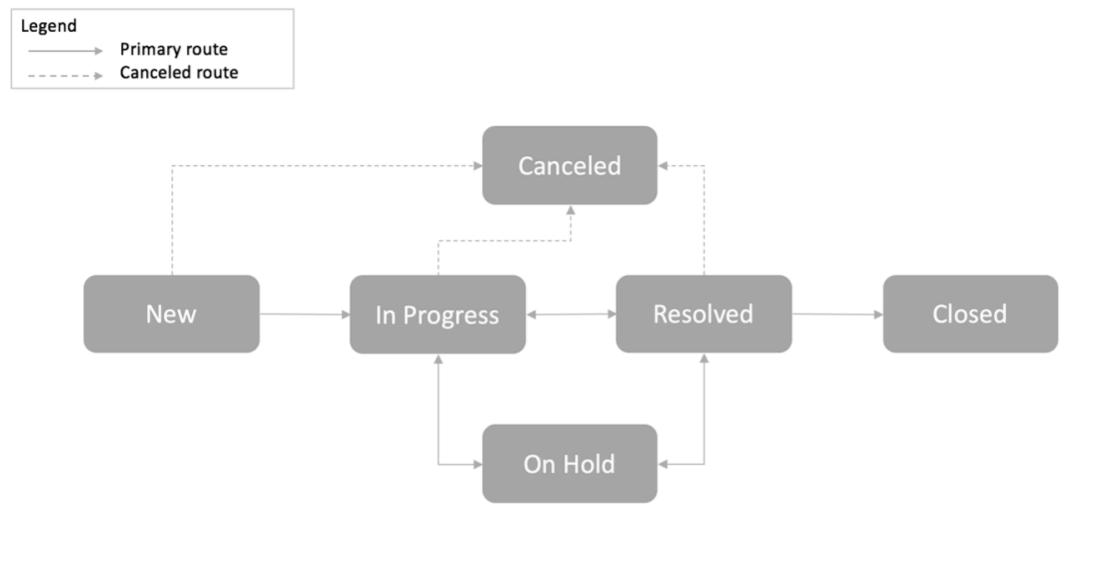
Operational Technology Incident Management

Operational Technology Incident Management enables engineers to quickly resolve Operational Technology (OT) device and production process issues.

Operational Technology Incident Management enables you to manage OT incidents separately from IT incidents. OT incidents occur when there's a disruption in service provided by an OT device on an OT network. Sometimes, the OT device may not be known when the incident is first created. If the OT device is unknown, an incident can be raised for an equipment model entity where the issue occurred.

The OT Incident manager is responsible for managing the default life cycle of incidents from creation to closure. The OT Incident Management process has many states, and each is important to the success of the process and the quality of service delivered. The different states are shown in the following diagram.

Operational Technology Incident Management process states



The incident states are as follows.

State	Description
New	Incident is logged but not yet investigated.
In Progress	Incident is assigned and being investigated.
On Hold	The responsibility for the incident temporarily shifts to another entity to provide further information, evidence, or a resolution. When you select the On Hold option, the reason list appears. If the On Hold reason is Awaiting

State	Description
	<p>Caller, the Additional comments section is required.</p> <p>i Note: If the caller updates the incident, the On Hold reason field is cleared and the state of the incident is changed to In Progress. An email notification is sent to the user whose name is mentioned in the Assigned to field and the users on the Watch list. You can place an incident On Hold one or more times before closing the incident.</p>
Resolved	An acceptable fix is provided for the incident to ensure that it doesn't happen again.
Closed	Incident is marked Closed after it's in the Resolved state for a specific duration, and it's confirmed that the incident is satisfactorily resolved.
Canceled	Incident was triaged but found to be a duplicate incident, an unnecessary incident, or not an incident at all.

Integrating with Industrial Process Manager

Integrate Operational Technology Incident Management with Industrial Process Manager to report incidents on equipment model entities.

Industrial Process Manager creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Operational Technology solution. When integrated with Operational Technology Incident Management, you're enabled to view incident impact against production processes.

The ISA Equipment Model plugin (`sn_isa_model`) installed with Industrial Process Manager enables views for specified roles. For more information, see [ISA-95 equipment model](#).

When an OT incident is created from an OT device record, the following occurs:

- The **OT device** field on the OT incident form is filled with the OT device value.
- If the OT device has an associated equipment model entity, then the equipment model entity is added to **Equipment model entity** field on the OT incident form.
- The **Site** field on the OT incident form is filled with the site of the OT device.

When an OT incident is created from an equipment model entity record, the following occurs:

- The **Equipment model entity** field on the OT incident form is filled with the equipment model entity value.
- The **Site** field on the OT incident form is filled with the site of the equipment model entity.

The **OT incident** related list on the equipment model entity record shows all OT incidents reported on that entity. The **Equipment model entity** field on the form can only have entities under the selected site.

Configuring Operational Technology Incident Management

Configure the Operational Technology Incident Management application so that you can create the data foundation for the ServiceNow® Operational Technology solution.

Operational Technology Incident Management v2 is dependent on Tokyo P5 or later.

i Note:

If you have the admin role, you can use the Guided Setup to lead you through the setup of the Operational Technology Incident Management application. To access the Guided Setup, navigate to **Industrial Workspace Admin > Guided Setup**.

Task	Purpose
1. Install the Operational Technology Incident Management application from the ServiceNow Store.	Installs the Operational Technology Incident Management application and supporting plugins.
2. Assign Operational Technology Incident Management roles.	Assigns roles to control the actions that are available for each user.
3. Migrate OT Incidents.	Migrates OT incidents from the incident table to the OT incident table. i Note: This step applies only when upgrading from Paris, San Diego, or Tokyo to Utah.
4. Configure categories and subcategories for OT incidents.	Configures categories and subcategories for OT incidents as needed.
5. Configure state models.	Configures state models for OT incident sites.
6. (Optional) Create an assignment rule.	Create an assignment rule to automatically assign an OT incident to the right group or user.

Install Operational Technology Incident Management

You can install the Operational Technology Incident Management application (`sn_ot_inc_mgmt`) if you have the admin role. The application installs related ServiceNow® Store applications and plugins if they are not already installed.

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](#).
- Operational Technology Incident Management requires the following plugins. Ensure that these plugins are activated before you install Operational Technology Incident Management.

Required ServiceNow plugins

CMDB CI Class Models (sn_cmdb_ci_class)

The CMDB CI Class Models store app adds class models that extend the CMDB class hierarchy, including class descriptions, identification rules, identifier entries, and dependent relationships. For more information, see [CMDB CI Class Models store app](#).

ISA Equipment Model (sn_isq_model)

The data model for ISA-95 equipment model entities and templates. For more information, see [ISA-95 equipment model](#).

- Operational Technology Incident Management requires either one or both of the following ServiceNow Store applications. Ensure that at least one of these applications is installed before you install Operational Technology Incident Management.

Required ServiceNow Store applications

Operational Technology Manager

The Operational Technology Manager application creates the foundational data and relationships that enables your enterprise to use the ServiceNow® Operational Technology solution. Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the Now Platform. For more information, see [Configuring the Operational Technology Manager](#).

Industrial Process Manager

The Industrial Process Manager application creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Industrial solution, enabling you to create your own version of the equipment models in each of your industrial sites. For more information, see [Configuring the Industrial Process Manager](#).

- Role required: admin

About this task

The following items are installed with Operational Technology Incident Management:

- Plugins
- Store applications
- Roles and ACLs

Note: For more information about the roles and ACLs installed, see [Components installed with Operational Technology Incident Management](#).

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Operational Technology Incident Management application (sn_ot_inc_mgmt) using the filter criteria and search bar.

You can search for the application by its name or ID. If you cannot find the application, you might 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.

Dependent plugins and applications are listed if they will be installed, are currently installed, or need to be installed. If any plugins or applications need to be installed, you must install them before you can install Operational Technology Incident Management.

4. Select **Install**.

Components installed with Operational Technology Incident Management

Several types of components may be installed with activation of the Operational Technology Incident Management (`sn_ot_inc_mgmt`) plugin, including user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see [Find components installed with an application](#).

Roles installed

Role	Description	Contains roles
OT Incident Admin [sn_ot_incident_admin]	Can create, view, delete and edit OT incident records for any equipment model entities. Can configure Priority Lookup Rules and OT incident system properties .	<ul style="list-style-type: none"> • cmdb_ot_isa_viewer_all • sn_ot_incident_write
OT Incident Reader [sn_ot_incident_read]	Can only view OT incident records.	<ul style="list-style-type: none"> • cmdb_ot_viewer • cmdb_ot_isa_viewer
OT Incident Fulfiller [sn_ot_incident_write]	Can view, create, and edit OT incident records.	sn_ot_incident_read

Note: The OT Incident User [`ot_incident_user`] role is deprecated. For users assigned this role, you can execute a scheduled job to assign them new Operational Technology Incident Management roles. For more information, see [Assign new roles to your users](#).

Tables installed

Table	Description
OT Incidents [sn_ot_incident]	List of OT incidents reported across sites.
OT Incident Tasks [sn_ot_incident_task]	List of OT incident tasks created under various OT incidents.

Table	Description
OT Incident Priority Rule Lookup [dl_ot_inc_priority]	List of rules to calculate the priority of an OT incident.

Migrate incidents to the new incident table

Migrate Operational Technology incidents from the old incident table to the new incident table. Migrating incidents lets the Operational Technology Incident Management application know that the old table is no longer applicable.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

Procedure

1. Navigate to **Industrial Workspace Admin > Guided Setup**.
2. In the Operational Technology Incident Management category, select **Get Started**.
3. Next to the Migrate OT Incidents section, select **Configure**.
4. Start the migration by selecting **Execute now**.
5. Optional: To see the activity log for this scheduled job, navigate to **All > System Logs > System Log > All**.

Result

The Operational Technology incidents are migrated to the new incident table, and the Operational Technology Incident Management application no longer uses the old table.

Assign roles to your users

Assign roles to your users in the Operational Technology Incident Management application so that you can control their access to the features, capabilities, and data.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the Operational Technology Incident Management application.

Note: The OT Incident User [ot_incident_user] role is deprecated. For users who are assigned with this role, you can execute the scheduled job "Assign New OT Incident Roles" to assign them with new Operational Technology Incident Management roles. For more information, see [Assign new roles to your users](#).

Role	Description
OT Incident Admin [sn_ot_incident_admin]	Can create, view, delete, and edit OT incident records for any equipment model entities. Users with this role can configure Priority Lookup Rules and OT incident system properties .

Role	Description
OT Incident Reader [sn_ot_incident_read]	Can only view OT incident records.
OT Incident Fulfiller [sn_ot_incident_write]	Can create, view, and edit OT incident records.

Procedure

Assign roles to users or groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Assign new roles to your users

Assign new roles to users who had the OT Incident User [ot_incident_user] role through a scheduled job in the Operational Technology Incident Management application.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

About this task

The OT Incident User role [ot_incident_user] is deprecated. You can assign new roles to users that had the ot_incident_user role through a scheduled script execution.

Procedure

1. Navigate to **All > System Definition > Scheduled Jobs**.
2. In the search bar, search for the **Assign New OT Incident Roles** scheduled job.
3. Start a scheduled job by selecting **Execute now**.
4. Optional: To see the activity log for this scheduled job, navigate to **All > System Logs > System Log > All**.

Result

The scheduled job is executed and users are now assigned with the new Operational Technology Incident Management roles.

Create an assignment group

Create an Operational Technology (OT) specific assignment group to assign to OT incident records.

Before you begin

Role required: admin

About this task

The **Assignment Group** field in an OT incident record only shows assignment groups with the type OT. This helps separate Operational Technology (OT) and Information Technology (IT) incidents.

You can create OT-specific assignment groups that you want visible on an OT incident record.

Procedure

1. Navigate to **All > User Administration > Groups**.
2. Select **New**.
3. On the form, fill in the fields.

Assignment groups form

Field	Description
Name	Name of the assignment group.
Manager	Group manager or lead.
Type	Category for this group. In the Select target record field, search for OT to add it to the type field.
Group email	Group email distribution list or the email address of the point of contact.
Parent	Other group that the group is a member of.
Description	Description of the assignment group.

4. Select **Submit**.

Result

Now, the OT-specific assignment group is visible on the incident record.

Incident categories and subcategories

By categorizing Operational Technology (OT) incidents, you can group and narrow the search for specific OT incidents.

When you can create an OT incident, you can choose from the categories and subcategories that are listed in the following table.

Incident categories

Category	Subcategory
Database	<ul style="list-style-type: none"> • DB2 • MS SQL Server • Oracle
Hardware	<ul style="list-style-type: none"> • OT issue • CPU

Incident categories (continued)

Category	Subcategory
	<ul style="list-style-type: none"> • Disk • Keyboard • Memory • Monitor • Mouse
Inquiry / Help	<ul style="list-style-type: none"> • Antivirus • Email • Internal Application
Network	<ul style="list-style-type: none"> • DHCP • DNS • IP Address • VPN • Wireless
Productivity	<ul style="list-style-type: none"> • Minor Stops • Slow Running • Setup and Adjustments • Breakdown
Quality	<ul style="list-style-type: none"> • Incoming Material • Startup Rejects • Process Defects - Qualitative • Process Defects - Quantitative
Safety	<ul style="list-style-type: none"> • Near Miss • Hazard • Safety Concern • Accident
Software	<ul style="list-style-type: none"> • Email • Operating System

Edit a category or subcategory

Edit your existing Operational Technology incident categories and subcategories to classify your incidents.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

Procedure

1. Navigate to **All > System Definition > Choice Lists**.
2. Set the condition filters to **[Table] [is] [sn_of_incident]** and **[Element] [is] [category]** or **[Element] [is] [subcategory]**.
3. Select the category or subcategory record.
4. Edit the form based on your needs.
5. Select **Save**.

Result

Now, the changes to the existing category or subcategory appear on the record.

Create a category or subcategory

Create an Operational Technology incident category or subcategory that you want to use to classify incidents.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

Procedure

1. Navigate to **All > System Definition > Choice Lists**.
2. To create a category, do these actions:
 - a. Select **New**.
 - b. In the **Element** field, enter the word **category**.
 - c. In the **Label** field, enter the category name.
 - d. In the **Value** field, enter the category value.
 - e. In the **Sequence** field, enter the sequence number.
 - f. Select **Submit**.
3. To add a new subcategory, do these actions:
 - a. Select **New**.
 - b. In the **Element** field, enter the word **subcategory**.
 - c. In the **Label** field, enter the subcategory name.
 - d. In the **Value** field, enter the subcategory value.
 - e. In the **Sequence** field, enter the sequence number.
 - f. Select **Submit**.

Result

The new category or subcategory is available to select on an Operational Technology incident record.

Delete a category or subcategory

Delete an Operational Technology incident category or subcategory if your organization no longer uses that category or subcategory.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

Procedure

1. Navigate to **All > System Definition > Choice Lists**.
2. Set the condition filters to **[Table] [is] [sn_ot_incident]** and **[Element] [is] [category]** or **[Element] [is] [subcategory]**.
3. Point to the category or subcategory record that you want to delete and select the check box.
4. In the Actions on selected rows menu, select **Delete**.

Result

The deleted category or subcategory is no longer available on an Operational Technology incident record.

Create an incident state model

Create an Operational Technology (OT) incident state model for your sites. By using an incident state model, you can manage the life cycle of the related incidents.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

About this task

By using state management, you can configure a state model for OT incident sites and their incident life cycles. You can create one model per site.

For more information about state management and state models, see [State Management](#).

For more information about the incident life cycles, see [Operational Technology Incident Management](#).

Procedure

1. Navigate to **All > State Management > State Models**.
2. Select the **OT Incident: Default Flow** model.
3. Set the **Condition**.
4. In the State Transitions Context menu, configure the State Transition records as required. For example, if you want to edit the **Enter Condition** field of the **In Progress** state record, select the state record, add your changes, and select **Update**.
5. Select **Update**.

Result

Now, the state model accurately describes the expected record workflow through the life cycle of the incident record.

Define a priority lookup rule for incidents

Define the impact and urgency of an Operational Technology incident to calculate its priority. You can then use the priority calculation to prioritize your work and to drive service level agreements (SLAs) in your organization.

Before you begin

Role required: ot_incident_admin

Procedure

1. Navigate to **All > Industrial Workspace Admin > Operational Technology Incident Management > Priority Lookup Rules**.
2. Select **New**.
3. On the form, fill in the fields.

Priority lookup rule form

Field	Description
Impact	Measure of the effect of an incident on business processes.
Urgency	Measure how long the resolution can be delayed until an incident has a significant business impact.
Priority	Option that is based on the impact and urgency. The priority identifies how quickly the OT engineer should address the task.
Application	Scope of the rules. The scope defines whether the rules are available for all applications or for scoped applications.
Active	Option to define whether the rule is active or not.
Order	Order in which the rules appear in the priority lookup list. This field indicates which rule to execute first.

Note:

The priority is calculated according to the sample data lookup rules in the following table.

Priority Data lookup rules

Impact	Urgency	Priority
1 - High	1 - High	1 - Critical
1 - High	2 - Medium	2 - High
1 - High	3 - Low	3 - Moderate
2 - Medium	1 - High	2 - High
2 - Medium	2 - Medium	3 - Moderate
2 - Medium	3 - Low	4 - Low
3 - Low	1 - High	3 - Moderate
3 - Low	2 - Medium	4 - Low
3 - Low	3 - Low	5 - Planning

By default, the **Priority** field is read-only and must be set by selecting the **Impact** and **Urgency** values. To change how the priority is calculated, you can either alter the priority lookup rules or disable the **Priority is managed by Data Lookup - set as read-only** UI policy and create their own business logic.

4. Select **Submit**.

Set the system properties

Set the system properties for the Operational Technology Incident Management application so that you can enable the incident properties as needed.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: sn_ot_incident_admin

Procedure

- Navigate to **All > Industrial Workspace Admin > Operational Technology Incident Management > System Properties**.
- Enable the following properties as needed for your organization.

Property	Description
com.sn_ot_inc_mgmt.sn_ot_incident_task-.closure	Property to close the open OT incident tasks when the related incident is closed or canceled.
com.snc.sn_ot_incident.create.child.enable	Property to create a child incident feature for the OT incident records.

Property	Description
com.snc.sn_ot_incident.copy.attributes	Property to list the attributes that you want to copy from the parent incident to the child incident.
glide.ui.sn_ot_incident_activity.fields	Fields that are visible in the activity formatter.

3. Select **Save** to save your changes.

Create an assignment rule

Create an assignment rule to automatically assign an Operational Technology (OT) incident to the right group or user according to one or more conditions in the assignment rule. Assignment rules are designed to run at the time you open an OT incident.

Before you begin

Role required: admin

Procedure

1. Navigate to **All > System Policy > Rules > Assignment**.
2. Select **New**.
3. On the form, fill in the following fields.

Assignment rule form

Field	Description
Name	Descriptive name for the assignment rule.
Active	Option to activate the assignment rule.
Applies to	
Table	<p>Table with the records that the assignment rule applies to.</p> <p>Note: For assignment rules specific to OT incidents, set the Table field to Operational Technology Incident [sn_ot_incident].</p> <p>The list shows only tables and database views that are in the same scope as the assignment rule. If you select a custom table that extends the task table, and for the assignment rule to work properly, you must clear the instance cache by navigating to <a href="https://<instance_name>.service-now.com/cache.do">https://<instance_name>.service-now.com/cache.do.</p> <p>Important: Clearing the system cache can affect overall performance, and degrade system response times. Do not run cache flushes during business hours, and do not trigger cache flushes automatically.</p>
Conditions	Conditions under which the assignment rule applies.
Assign to	
User	User the event is assigned to.

Field	Description
Group	Group the event is assigned to.
Script	<p>Script to specify advanced assignment rule functionality. The current.variable_pool set of variables is available.</p> <p>i Note: Make sure the input in the script is correct, and that the input type matches the field type in the Assignment Rule script. For example, if the assignment rule script sets the value of an Integer field, and the value in the script is set to String, the assignment rule may yield unexpected results.</p>
Optional fields	
Match conditions	<p>Any If any of the conditions are met, assignment rule applies.</p> <p>All If all the conditions are met, assignment rule applies.</p>
Execution Order	Order in which the assignment rule is processed. If assignment rules conflict, a rule with a lower-order value takes precedence over a rule with a higher value. If the order values are set to the same number, the assignment rule with the first matching condition takes precedence over the others. Only the first assignment rule with a matching condition runs against a record.

4. Select **Submit**.

What to do next

For more information about assignment rules, see [Define assignment rules](#).

Using Operational Technology Incident Management

After you complete all required set up tasks for the Operational Technology Incident Management application, you can begin managing OT incidents.

Managing OT incidents

Depending on your assigned user role, you can manage OT incidents in the Industrial Workspace.

In the Industrial Workspace, the OT incident writer can create and update an OT incident form from the following places:

- An OT device form
- An equipment model entity form
- The List module

In the Industrial Workspace, the OT incident viewer can view OT incidents in the following places:

- The "OT incidents" related list on the OT device form
- The "OT incidents" related list on the OT device form on the equipment model entity form
- The following lists on the List module:

- Assigned to me
- Belong to my sites
- All

The OT incident admin can go to any OT incident record in the Industrial Workspace and delete it.

Access control for incidents

To help separate Operational Technology (OT) and Information Technology (IT) data, only OT users can view OT incidents.

The following table describes the roles and permissions for the users that have the Operational Technology Incident Management roles.

Role	Permissions
sn_ot_incident_write	Can create, edit, and read OT incidents.
sn_ot_incident_read	Can only read OT incidents.
sn_ot_incident_admin	Can create, view, edit, and delete incident records for any equipment model entity.

For more information about access control rules, see [Access control rules in application administration apps](#).

Report an incident

Create an Operational Technology (OT) incident record to report a deviation from an expected standard of operation.

Before you begin

Role required: sn_ot_incident_write

Procedure

1. Navigate to **All > Industrial Workspace**.
2. Select an device record or an equipment model entity record.

i Note: You can also raise an OT incident on the OT Incidents list module.

3. Select the **OT Incidents** tab.

4. Select **New**.

5. On the form, fill in the fields.

If you selected an device record, the Site and OT device fields are automatically filled in.

If you selected an equipment model entity record, the Site and Equipment model entity fields are automatically filled in. If the OT incident is raised from the OT Incidents list module, then none of these fields are automatically filled in.

i Note: Your organization has configured the incident form and its fields to adhere to its incident management process. The following table describes the typical OT incident form fields.

Operational Technology incident form

Field	Description
Short description	Brief description of the incident.
Description	Detailed explanation of the incident.
Number	Unique system-generated incident number that is prefixed with Operational Technology Incident (OTINC).
Caller	User who contacted the OT engineer with an issue.
Impact	Measure of the effect that an incident has on industrial processes.
Urgency	Measure of how long the resolution can be delayed until an incident has a significant business impact.
State	State of the OT incident. The state moves and tracks incidents through several stages of resolution.
Category	Type of issue. After selecting the category, select the subcategory if applicable.
Subcategory	Type of issue within the selected category.
Watch list	Users who receive notifications about this incident when comments are added.
Work notes list	Users who receive notifications about this incident when work notes are added.
Site	Site where the issue happened.
OT device	Affected OT device at the site.
Equipment model entity	Affected equipment model equipment model entity at the site.
Business impact	More information about the business impact of the OT incident.
Assignment group	Assigned group that works on the incident. The assignment group can be any group with the type OT.
Assigned to	<p>User who works on this incident. If the assignment group changes, the Assigned to field is cleared.</p> <p>You can only select the users that are included in the Assignment group field and have the sn_ot_incident_write role. If the Assignment group field is empty, then any site user with the sn_ot_incident_write role can be selected.</p>

Field	Description
Parent incident	Unique number of the parent incident for this incident record.
Additional comments	More information about the issue as needed. All users that can view incidents can see the additional comments.
Work notes	Information about how to resolve the incident or the steps taken to resolve it, if applicable.

6. Select **Save**.

Result

Now, the assignment group and assignee are aware that there's an OT incident that needs to be addressed.

Create tasks to fulfill an incident

Create a set of incident tasks to fulfill an Operational Technology (OT) incident. Incident tasks help you to split up and categorize the work that is needed to resolve an incident.

Before you begin

Role required: sn_ot_incident_write

Procedure

1. Navigate to **All > Incident > Open**.
2. Open the OT incident record that you want to create a task for.
3. In the Incident Tasks related list, select

The screenshot shows a list of 'Operational Technology Incident Tasks'. The header includes filters for 'Number' and 'Search', and columns for 'Short description', 'Priority', 'State', 'Assignment group', 'Assigned to', 'Updated', and 'Updated by'. Below the header, there is a message 'No records to display' next to a small icon of a computer monitor with a circular arrow. The 'New' button in the top right corner of the list area is highlighted with a red box.

New.

If you don't see the Incident Tasks related list, you must add it.

4. On the form, fill in the

The screenshot shows the ServiceNow interface for an Operational Technology Incident. The main form has fields for Short description, Description, Number (OTINC000004), Caller (all_admin), Category (Hardware), Subcategory (OT Issue), State (In Progress), Impact (2 - Medium), Urgency (2 - Medium), Priority (3 - Moderate), and Watch list. Below this is a sub-form for Impact with fields for Site (site1), Equipment model entity (st1), and OT asset. At the bottom is a list of Child Incidents.

fields.

Incident task form

Field	Description
Number	Unique system-generated incident task number.
Incident	Incident with which the task is related.
Site	Affected incident site. i Note: This field is read-only and is automatically filled in with the related incident site, if applicable.
Equipment Model Entity	Affected equipment model entity. i Note: This field is read-only and is automatically filled in with the related equipment model entity, if applicable.
OT device	Affected OT device. i Note: This field is read-only and is automatically filled in with the related OT device, if applicable.
State	State for tracking an incident task through several stages of the incident's resolution.
Priority	Priority of the incident task.
Assignment group	Group who works on the incident task. If you leave this field empty, the incident is automatically assigned.
Assigned to	User to whom the incident task is assigned to work on.

Field	Description
	i Note: If the Assignment group changes, the Assigned to field is cleared.
Short description	Brief description of the incident task.
Description	Detailed explanation on the incident task.
Notes	<p>Work notes list</p> <p>Users who receive notifications about this incident task when work notes are added.</p> <p>i Note: You can select the add me icon  to add yourself to the work notes list.</p>
Work notes	Information about how to resolve the incident task, or the steps that need to be taken to resolve it, if applicable.

5. Select **Submit**.

Result

Now, you can view and edit the incident task in the related OT incident record.

You can view incident tasks in the Industrial Workspace list view in the following places.

- Incident tasks assigned to you: **OT Tasks > Assigned to Me**
- Incident tasks assigned to your group: **OT Tasks > Assigned to My Groups**
- Unassigned incident tasks: **OT Tasks > Unassigned**

Create a child incident

Create a child Operational Technology (OT) incident record to capture part of the deviation reported so that it can be worked on separately. Creating child incidents can help you organize multiple incidents related to the same parent.

Before you begin

- Enable the Create child incident feature (`com.snc.incident.create.child.enable`) property. For more information, see [Set the system properties](#).
- Role required: `sn_ot_incident_write`

About this task

Fields that are copied over to the child incident are configured by using the `com.snc.sn_ot_incident.copy.attributes` system property.

Procedure

1. Navigate to the **OT Incidents** list module in the Industrial Workspace. Alternatively, you can go to an OT device record or equipment model entity record and select the **OT Incidents** tab.
2. Open the OT incident that you want to create a child incident for.

3. Select the **Child Incidents** related list.

4. Select **New**.

5. Fill in the details of the child incident.

6. Select **Save**.

Result

Now, you can view and edit the child incident in the parent incident record.

Visibility of incidents across sites

With the Operational Technology (OT) incident fulfiller role (`sn_ot_incident_write`), you can view, create, or edit the incidents that belong to your site. You can also view the incidents that belong to other sites to help resolve similar incidents at your site.

Overview

If you're a user with the OT incident fulfiller role (`sn_ot_incident_write`), you can do the following tasks:

- View and edit the OT incident records that are assigned to you or the incidents that belong to your site.
- Create OT incidents.
- View OT incidents that belong to the other sites.

Benefit of the OT incident fulfiller role

The main benefit of being an OT incident fulfiller is that you have read-only visibility of incidents across sites. Viewing other incidents across sites can help you resolve similar incidents at your site.

Note: You can't edit OT incidents for other sites. You can only edit incidents that belong to your site.

Where to view or edit incidents

The following OT incident lists are available in the Lists module on the Industrial Workspace:

- Assigned to me: View and edit your assigned incident records by navigating to **OT Incidents > Assigned to me**.
- Belong to my sites: View and edit the incident records that belong to your sites by navigating to **OT Incidents > Belong to my sites**.
- View the existing incident records at different sites by navigating to **OT Incidents > All**.

Synchronization between an incident and its incident tasks

You can use Operational Technology (OT) incident tasks to collaborate with and request work from other stakeholders. An OT incident and its tasks are synchronized so that the state of the incident tasks change depending on the state of incident.

The `com.snc.incident.ot_incident_task.closure` property closes open incident tasks when the related incident is closed or canceled. This property is responsible for different actions that take place on OT incident tasks based on the state of the OT incident.

The synchronization between an OT incident and its open OT incident task is as follows:

- When an OT incident is closed, the state of any open OT incident task is set to **Closed Incomplete**.
- When an OT incident is canceled, the state of any open OT incident task is set to **Closed Skipped**.

Incident email notifications

Use Operational Technology (OT) incident email notifications to alert users when changes are made to an incident.

The notifications are listed in the following table.

OT incident email notifications

Notification name	When to send	Who receives it	What it contains
Incident commented	When an extra comment is added	Assigned to, Watch list	Subject: <Incident #> - comment added Body: Comment added URL to the incident
Incident opened and unassigned	When the Assigned to field changes to empty and Active is true	The one who opened the incident	Subject: <Incident #> - is unassigned Body: Please identify someone to work on this incident URL to the incident
Incident closed	When the incident is closed	Assignment group	Subject: <Incident #> - is closed Body: Resolution Code and Resolution Notes
Incident priority changed	When triggered	Assigned to, Assignment group, Watch list	Subject: <Incident #> - priority changed Body: New priority: <priority>
Incident resolved	When the incident state changes to Resolved	Caller, Watch list	Subject: <Incident #> - is resolved Body: Resolution Code and Resolution Notes

OT incident email notifications (continued)

Notification name	When to send	Who receives it	What it contains
Incident assigned to my group	When the Assignment Group field changes	Assignment group, Watch list	Subject: <Incident #> - is assigned to <assignment group> Body: Priority, Short description, Description URL to the incident
Incident assigned to me	When the Assigned to field changes	Assigned to, Watch list	Subject: <Incident #> - is assigned to you Body: Priority, Short description, Description URL to the incident
Incident opened for me	When a new incident is created	Caller	Subject: <Incident #> - is opened on your request Body: Priority, Short description, Description URL to the incident
Incident state changed	When the state of the incident changes	Assigned to, Watch list	Subject: <Incident #> - State changed Body: Short description, Old State, New State URL to the incident

Compose an email from an OT incident record

Compose an email directly in an OT incident record to conveniently update your team and others required about the incident.

Before you begin

Role required: sn_ot_incident_write

Procedure

1. Navigate to **All > Industrial Workspace**.
2. Open the Industrial Workspace list view.

3. Under the **OT Incidents** list module, select one of the available lists.
4. Select the incident record that you want to send an email for.
5. Select the **More actions**  button in the incident header to open the menu.
6. Select **Compose Email**.
7. On the email template, fill in the following fields.

Email template fields

Field	Description
To	User or users you want to send the email to. This field automatically populates with the user in the Assigned to field of the OT incident record.
Subject	Subject of the email. This field automatically populates with the number of the OT incident record and its short description.
Body	Updates that you want to send to a user or users related to the OT incident.

8. Optional: If the email is a response, you can use the **Response Templates** available to fill in the email body.
9. Optional: To save the email as a draft, select **Save as draft**.
10. Select **Send Email**.

Result

The email is sent to the user or users you specified in the email template.

Resolve and close an incident

When an issue is corrected, you can set the Operational Technology (OT) incident state to **Resolved**. If you're happy with the resolution, you can close the incident. The incident also auto-closes after a certain amount of time based on the incident auto-close properties.

Before you begin

Role required: sn_ot_incident_write

Procedure

1. Navigate to **All > Incident > Open**.
2. Open the OT incident that you want to resolve and close.
3. In the **Resolution Information** related list, fill in the following fields.

Resolution Information fields

Field	Description
Resolution code	Information to categorize resolved cases.

Field	Description
Resolution notes	Describes how the incident was resolved.

4. Click **Update.**

Edit related devices and equipment model entities in an incident record

Add or remove related Operational Technology (OT) devices and equipment model entities directly from an OT incident record, which can help you keep track of the relationship between the incident and its effected items.

Before you begin

Role required: sn_ot_incident_write or sn_ot_incident_admin

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the **OT Incidents** module list view, select one of the available lists.
3. Select the incident record that you want to add or remove a related device or equipment model entity from.
4. To add a related OT device from the incident record, do these actions:
 - a. Select the **Affected OT Devices** related list.
 - b. Select **Add**.
 - c. In the **Add OT Devices** window, select the check boxes next to the devices that you want to add.
 - d. Select **Add**.

The OT devices are now added to the incident record under the Affected OT Devices related list.
5. To remove a related OT device from the incident record, do these actions:
 - a. Select the Affected OT Devices related list.
 - b. Select the check boxes next to the devices that you want to remove.
 - c. Select the **Remove** button. A confirmation window appears asking if you want to proceed.
 - d. Select **Remove** in the window to continue.

The OT device or devices are removed from the incident record and the Affected OT Devices related list.
6. To add or remove an equipment model entity from an incident record, repeat steps 4 and 5 but under the Impacted Equipment Model Entities related list.

Operational Technology Incident Management reference

Reference topics provide additional information about the Operational Technology Incident Management application.

Related information

For more information about the Operational Technology (OT) product view related to the Common Service Data Model (CSDM), the Network Intrusion Detection System (NIDS), OT extension classes, and related applications see the following.

Overview

The product view and the extension classes help you understand how Operational Technology Management works with the CSDM framework and the Configuration Management Database (CMDB) respectively.

[Operational Technology product view](#)

The Operational Technology product view helps you understand how Operational Technology key entities work with the CSDM framework.

[Operational Technology \(OT\) extension classes](#)

The Configuration Management Database (CMDB) updates classes for OT.

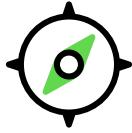
Related applications

[IT Service Management](#)

When integrated with Operational Technology Incident Management, the ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Operational Technology Change Management

The ServiceNow® Operational Technology Change Management application enables your organization to implement changes to Operational Technology (OT) devices and production processes.

<p>Explore</p>  <p>Exploring Operational Technology Change Management</p>	<p>Configure</p>  <p>Plan and configure your implementation</p>
<p>Use</p>  <p>Using Operational Technology Change Management</p>	<p>Reference</p>  <p>Get details about related information and applications</p>

Exploring Operational Technology Change Management

Learn more about the Operational Technology Change Management application.

Key features

With the Operational Technology Change Management application, you can use the following key features:

- Digitized change workflow that connects all stakeholders.
- Sites that have different change management processes (workflows).
- Separated IT Change Management and Operational Technology Change Management, but ability to be combined if necessary.
- Integrated Operational Technology Change Management workflow with the Operational Technology Incident Management and Operational Technology Vulnerability Response applications.
- Aligned factory floor changes for the equipment model entities with downtime schedules.

Using Operational Technology Change Management to optimize your production process

The Operational Technology Change Management application enables your team members to work collaboratively on changes to operational technology (OT) devices or industrial equipment configurations. These changes include any optimizations, alterations in the production process, or vulnerability fixes.

Overview

By using the Operational Technology Change Management application, you can manage your OT change requests separately from your Information Technology (IT) change requests. You can separate OT change requests from IT change requests by the network type and you can manage OT change requests per site.

The following examples show how to apply Operational Technology Change Management to your organization:

- An OT remediation owner, who's responsible for fixing vulnerabilities on OT devices, wants to initiate a change to fix a group of vulnerabilities.
- An OT technician, who's responsible for OT configurations and plant engineering activities, wants to execute a change to fix a malfunctioned robotic arm on the industrial floor.
- A plant head, who's responsible for overall production activity, wants to review and approve a change requested by the engineering team.

OT change requests

OT change requests occur when there's a disruption in service from an OT device on an OT network. In some cases, the OT device may not be known when the change request is created. When you create an OT change request from the Industrial Workspace, the change request is automatically assigned a Network Type of **OT**. This attribute is used to distinguish an OT change request from an IT change request. This field isn't displayed by default. For more information about OT devices, see [OT device related items and related lists](#).

For more information about how to create an OT change request, see [Create a change request](#).

Separating an IT and OT change

When the Operational Technology Change Management application is installed on your instance, you can choose a Network Type of **IT**, **OT**, or **None**. New change requests are assigned a Network Type of **None** by default.

Operational Technology Change Management model state transitions

The following tables list the Operational Technology Change Management model state transitions for both the Basic OT Change Model and the Advanced OT Change Model. For more information about the OT Change Models, see [Select a change model to fulfill change requests](#).

States for the Basic OT Change Model

State	Description
New	An OT change request is initiated.
Plan	<p>The OT change request is analyzed with the following criteria:</p> <ul style="list-style-type: none"> • Justification • Implementation plan • Risk and impact analysis • Backout plan • Test plan • Schedule the change
Implementation	The change is performed on the targeted OT device.
Closed	The change record is closed after the change is completed.
Canceled	The change record is canceled and the change isn't applied to the OT device.

States for the Advanced OT Change Model

State	Description
New	An OT change request is initiated.
Plan	<p>The OT change request is analyzed with the following criteria:</p> <ul style="list-style-type: none"> • Justification • Implementation plan • Risk and impact analysis • Backout plan • Test plan • Schedule the change

States for the Advanced OT Change Model (continued)

State	Description
Approve	The reviewers approve or deny the OT change request.
Implementation	The change is performed on the targeted OT device.
Post-Implementation Review	Add additional OT change tasks if needed and perform the following checks: <ul style="list-style-type: none"> • Electrical check • Network check • Quality check • Safety check
Closed	The change record is closed after the change is completed.
Canceled	The change record is canceled and the change isn't applied to the OT device.

Configuring Operational Technology Change Management

Configure the Operational Technology Change Management application so that you can create the data foundation for the ServiceNow® Operational Technology (OT) solution.

If you have the admin role, you can use the Guided Setup to lead you through the setup of the Operational Technology Change Management application. Guided Setup is a tool that assists with application configuration. It organizes the configuration activities into categories. These categories contain the information about the setup tasks, steps to complete each task, and links to the pages in your instance where you perform the configuration. Links to useful help content are also provided.

 Note:

Operational Technology Change Management is dependent on Utah P4 or later releases.

To access the Guided Setup, navigate to *Industrial Workspace Admin > Guided Setup*.

The following table explains the Guided Setup tasks and their purpose for the Operational Technology Change Management application.

Task	Purpose
1. Install the Operational Technology Change Management application from the ServiceNow Store.	Installs the Operational Technology Change Management application and supporting plugins.
2. Assign Operational Technology Change Management roles.	Assigns the roles to control the actions that are available for each user.

Task	Purpose
3. Configure Operational Technology Change Management categories.	Configures the categories for the OT changes that are needed for your organization.
4. Select the Operational Technology Change Management model.	Selects the change model for your organization.

Install Operational Technology Change Management

You can install the Operational Technology Change Management application (`sn_ot_chg_mgmt`) if you have the admin role.

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](#).
- The Operational Technology Change Management application requires the following plugins. Ensure that these plugins are activated before you install the Operational Technology Change Management application.

Required ServiceNow plugins

CMDB CI Class Models (`sn_cmdb_ci_class`)

The Configuration Management Database (CMDB) CI Class Models store app adds class models that extend the CMDB class hierarchy, including the class descriptions, identification rules, identifier entries, and dependent relationships. For more information, see [CMDB CI Class Models store app](#).

ISA Equipment Model (`sn_isa_model`)

The data model for ISA-95 equipment model entities and templates. For more information, see [ISA-95 equipment model](#).

- The Operational Technology Change Management application requires either one or both of the following ServiceNow Store applications. Ensure that at least one of these applications is installed before you install the Operational Technology Change Management application.

Required ServiceNow Store applications

Operational Technology Manager

The Operational Technology Manager application creates the foundational data and relationships that enable your organization to use the Operational Technology solution. The Operational Technology Manager application supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the Now Platform. For more information, see [Configuring the Operational Technology Manager](#).

Industrial Process Manager

The Industrial Process Manager application creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Industrial solution, enabling you to create your

own version of the equipment models in each of your industrial sites. For more information, see [Configuring the Industrial Process Manager](#).

Role required: admin

About this task

The following items are installed with the Operational Technology Change Management application:

- Plugins
- Store applications
- Roles and ACLs

i Note: For more information about the roles and ACLs installed, see [Components installed with Operational Technology Change Management](#).

Procedure

1. Navigate to **All > System Applications > All Available Applications > All**.
2. Find the Operational Technology Change Management application by 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 might 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. Dependent plugins and applications are listed if they'll be installed, are currently installed, or must be installed. If any plugins or applications must be installed, you must install them before you can install the Operational Technology Change Management application.
4. Select **Install**.

Components installed with Operational Technology Change Management

Several types of components may be installed with activation of the Operational Technology Change Management (sn_ot_chg_mgmt) application, including the user roles.

i Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see [Find components installed with an application](#) .

Roles installed

Role	Description	Contains roles
Change Manager [sn_ot_change_manager]	Can manage OT change model records.	<ul style="list-style-type: none"> • sn_ot_change_write • sn_stfrm_condition_read

Role	Description	Contains roles
Change Admin [sn_ot_change_admin]	Can create, view, delete, and edit OT change records. Can configure categories and system properties.	<ul style="list-style-type: none"> cmdb_ot_isa_viewer_all sn_ot_change_write
Change Write user [sn_ot_change_write]	<p>Can create, view, and edit OT change records.</p> <p>Can also be assigned IT change tasks, and can edit and close the IT change task they're assigned to.</p> <p>For more information, see Managing change requests across sites.</p>	<ul style="list-style-type: none"> cmdb_ot_viewer cmdb_ot_isa_viewer sn_ot_change_read
Change Read user [sn_ot_change_read]	Can only view OT change records.	<ul style="list-style-type: none"> cmdb_ot_viewer cmdb_ot_isa_viewer

Assign Operational Technology Change Management roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Operational Technology Change Management application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the application.

Role	Description
Change Manager [sn_ot_change_manager]	Can manage OT change model records.
Change Admin [sn_ot_change_admin]	Can create, view, delete, and edit OT change records. Can configure categories and system properties.
Change Write user [sn_ot_change_write]	<p>Can create, view, and edit OT change records.</p> <p>Can also be assigned IT change tasks, and can edit and close the IT change task they're assigned to.</p> <p>For more information, see Managing change requests across sites.</p>
Change Read user [sn_ot_change_read]	Can only view OT change records.

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Change categories

By categorizing the Operational Technology (OT) change requests, you can group and narrow the search for specific OT change requests. Categories also help stakeholders know what the change is about.

When you can create an OT change request, you can choose from the categories listed in the following table.

OT change request categories

Category	Description
Hardware	Changes to add, remove, or configure OT devices.
Software	Changes to add, remove, or configure OT software.
Service	Changes to an OT service.
System Software	Changes to the OT system software.
Applications Software	Changes to the OT applications software.
Network	Changes to subnets, IP addresses, and MAC addresses.
Telecom	Changes to telecommunications used in your OT system.
Documentation	Changes to the OT documentation.
Firmware	Changes to the OT firmware.
Other	Other changes not captured in the categories above.

Select a change model to fulfill change requests

Select an Operational Technology (OT) change model to begin fulfilling your change requests depending on the needs of your organization.

Before you begin

Role required: sn_ot_change_admin or admin

About this task

Two OT change models are available for you to use:

- OT Change Basic
- OT Change Advanced

The OT Change Basic model uses the change process without approvals.

For more information about the OT Change Basic Model, see [Basic OT Change Model playbook](#).

The OT Change Advanced model uses the change process with approvals. You can create a change approval policy and assign an approval group to review your change request. For more information about change approvals, see [Operational Technology change approval](#).

For more information about the Advanced OT Change Model, see [Advanced OT Change Model playbook](#).

Procedure

1. Navigate to **Industrial Workspace Admin > Guided Setup**.
2. In the Operational Technology Change Management category, select **Get Started**.
3. Next to the Change Models section, select **Configure**.
4. Select the change model that fits the needs of your organization.
5. Edit the record as needed.

Result

The change model is applied to your system and you can begin creating OT change requests.

Basic OT Change Model playbook

Learn about the Basic Operational Technology (OT) Change Model playbook stages that an OT change without approvals must go through until it's completed.

Initiate

The Initiate stage of an OT change request lets you capture the details of the requested change and assign the change as necessary. This stage has three tasks.

Describe the change

Field	Description
Short description	Brief description of the change.
Description	Details of the change.
Category	Type of change.
Site	Site where the change takes place.
Watch list	Users who receive notifications about this change when comments are added.
Work notes list	Users who receive notifications about this change when work notes are added.

Capture risk

Field	Description
Priority	Impact and urgency to identify how quickly the change should be addressed.
Risk	Amount of risk that the change poses.

Capture risk (continued)

Field	Description
Impact	Measure of the effect that a change has on your industrial processes.

Assign the change

Field	Description
Requested by	User who requests the change.
Assignment group	Assigned group that works on the change. The assignment group can be any group with the type OT.
Assigned to	User who works on this change. If the assignment group changes, the Assigned to field is cleared.

Plan

The Plan stage of an OT Change request lets you add a justification for the change, an implementation plan, a risk and impact plan, a backout plan, a test plan, and a time to schedule the change. This stage has six tasks.

Add a justification

Field	Description
Justification	Reason why the change must take place.

Add implementation plan

Field	Description
Implementation plan	Details of how to implement the requested change.

Add risk and impact analysis

Field	Description
Risk and impact analysis	Details of any risk and impact factors that are related to this change.

Add backout plan

Field	Description
Backout plan	Details of how to reverse the change in place if necessary.

Add test plan

Field	Description
Test plan	Details of how to test the implemented change.

Schedule the change

Field	Description
Planned start date	Date that the change takes place. i Note: You can also choose an available downtime slot on the calendar by selecting the Scheduling Assistant button to fill in the planned start date field automatically.
Planned end date	Date that the change ends. i Note: You can also choose an available downtime slot on the calendar by selecting the Scheduling Assistant button to fill in the planned end date field automatically.

Implement

The Implement stage of an OT change request provides the details of the following task. You can mark this stage as complete when it's finished.

Perform the change

Mark as complete when the change is performed on the targeted OT devices and completed.

Close

The Close stage lets you close the change record after the change is completed.

Close the change record

Field	Description
Close code	Reason that the change record was closed.
Close notes	Additional details about closing the change record.

Advanced OT Change Model playbook

Learn about the Advanced Operational Technology (OT) Change Model playbook stages that an OT change with approvals must go through until it's completed.

Initiate

The Initiate stage of an OT Change request lets you capture the details of the requested change and assign the change as necessary. This stage has three tasks.

Describe the change

Field	Description
Short description	Brief description of the change.
Description	Details of the change.
Category	Type of change.
Site	Site where the change takes place.
Watch list	Users who receive notifications about this change when comments are added.
Work notes list	Users who receive notifications about this change when work notes are added.

Capture risk

Field	Description
Priority	Impact and urgency to identify how quickly the change should be addressed.
Risk	Amount of risk the change poses.
Impact	Measure of the effect that a change has on your industrial processes.

Assign the change

Field	Description
Requested by	User who requests the change.
Assignment group	Assigned group that works on the change. The assignment group can be any group with the type OT.
Assigned to	User who works on this change. If the assignment group changes, the Assigned to field is cleared.

Plan

The Plan stage of an OT change request lets you add a justification for the change, an implementation plan, a risk and impact plan, a backout plan, a test plan, and a time to schedule the change. This stage has six tasks.

Add justification

Field	Description
Justification	Reason why the change must take place.

Add implementation plan

Field	Description
Implementation plan	Details of how to implement the requested change.

Add risk and impact analysis

Field	Description
Risk and impact analysis	Details of any risk and impact factors that are related to this change.

Add backout plan

Field	Description
Backout plan	Details of how to reverse the change in place if necessary.

Add test plan

Field	Description
Test plan	Details of how to test the implemented change.

Schedule the change

Field	Description
Planned start date	Date that the change takes place. i Note: You can also choose an available downtime slot on the calendar by selecting the Scheduling Assistant button to fill in the planned start date field automatically.
Planned end date	Date that the change ends. i Note: You can also choose an available downtime slot on the calendar by selecting the Scheduling Assistant button to fill in the planned end date field automatically.

Approve

The Approve stage of an OT Change request lets reviewers approve or deny the OT Change. This stage includes only one task.

Review and take action

Field	Description
Approve button	If you're a reviewer shown in the table on the task form, select Approve to accept the change.
Deny button	If you're a reviewer shown in the table on the task form, select Deny to reject the change.
Comments	Additional information about the approval or denial of the change.

For more information about change approvals, see [Operational Technology change approval](#).

Implement

The Implement stage of an OT change request provides the details of the following tasks. You can mark this stage as complete when it's finished.

Stop the function

If needed, mark as complete after you stop the function of the targeted OT devices.

Ensure LOTO

Lockout/Target (LOTO) is a safety procedure to prevent accidental or unintentional start-up of machinery during maintenance or service. Mark as complete when LOTO is completed.

Perform the change

Mark as complete when the change is performed on the targeted OT devices and completed.

Post-implementation Review

The Post-implementation Review stage of an OT change request lets you check off the performed tasks, create additional OT change tasks for remaining work identified during the review, and mark the revoke LOTO process as complete.

Perform checks

Field	Description
Perform electrical check	Check box that you select after the electrical check has been completed.
Perform network check	Check box that you select after the network check has been completed.
Perform quality check	Check box that you select after the quality check has been completed.
Perform safety check	Check box that you select after the safety check has been completed.

Recommend spin-off tasks

Field	Description
OT Change Tasks	List of the change tasks that are related to the OT change.
State	State of the OT change. The state moves and tracks changes through several stages of resolution.
Assigned to	User who works on this change. If the assignment group changes, the Assigned to field is cleared.
Short description	Brief description of the change task.

Revoke LOTO

After the change is implemented and reviewed, mark as complete when the lockout-target is revoked.

Spin-off Tasks

The Spin-off Tasks stage lists all the change tasks in the Post Implementation Review that must be completed.

Close

The Close stage lets you close the change record after the change is completed.

Close change record

Field	Description
Close code	Reason that the change record was closed.
Close notes	Additional details about closing the change record.

Using Operational Technology Change Management

After you complete all required set-up tasks for the Operational Technology Change Management application, you can begin managing Operational Technology (OT) change requests.

Create a change request

Create an Operational Technology (OT) change request to report a change in your site.

Before you begin

Role required: sn_ot_change_write

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the **OT Change Requests** list view, select the list you want to open.
3. Select **New**.

4. Select the OT change model that applies to your organization.
5. Select **Create OT Change Record**.
6. Complete the playbook as needed as your team works on the change request.
For more information about the Basic OT Change Model playbook, see [Basic OT Change Model playbook](#). For more information about the Advanced OT Change Model playbook, see [Advanced OT Change Model playbook](#).

Create a change task to fulfill a change request

Create a change task to fulfill an Operational Technology (OT) change request. Change tasks help to capture all the tasks that need to take place during a change request.

Before you begin

Role required: sn_ot_change_write

About this task

Change tasks are the individual steps that must take place to fulfill and complete a change request.

Procedure

1. Navigate to **All > Industrial Workspace**.
2. Select the change record that you want to create a task for.
3. In the Change Tasks related list, select **New**.
If you don't see the Change Tasks related list, you must add it.
4. On the form, fill in the fields.

Incident task form

Field	Description
OT Change Task	
Short description	Brief description of the change task.
Description	Details of the change task.
OT device	Affected OT device.
OT change request	Record number of the related OT change request.
State	State for tracking a change task through several stages of the change implementation.
Type	Type of change.
Assignment	
Assignment group	Group who works on the change task. If you leave this field empty, the change task is automatically assigned.
Assigned to	User to whom the change task is assigned to work on.

Field	Description
OT Change Task	<p>Note: If the Assignment group changes, the Assigned to field is cleared.</p>
Notes	
Watch list	Users who receive notifications about this change when comments are added.
Work notes list	Users who receive notifications about this change when work notes are added.
Work notes (Private)	Work notes that aren't available to customers.

5. Select **Save**.

Result

You can view and edit the change task in the related OT change record.

You can view change tasks in the Industrial Workspace list view in the following places.

- Change tasks assigned to you: **OT Tasks > Assigned to Me**
- Change tasks assigned to your group: **OT Tasks > Assigned to My Groups**
- Unassigned change tasks: **OT Tasks > Unassigned**

Create a change request from OT device details

Create an Operational Technology (OT) change request from an OT device record. Creating a change request from a device record automatically populates the information in your change request record, such as the site or business service and the OT Device field.

Before you begin

Role required: sn_ot_change_write

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the All OT Devices list, select an OT device record.
3. In the record, select the OT Change Requests related list.
4. Select **New**.
5. Select the OT change model that applies to your organization.
6. Select **Create OT Change Record**.
7. Complete the playbook as needed as your team works on the change request.

For more information about the Basic OT Change Model playbook, see [Basic OT Change Model playbook](#). For more information about the Advanced OT Change Model playbook, see [Advanced OT Change Model playbook](#).

The following fields are automatically populated depending on the conditions that you set.

- The **OT Device** field is auto-populated only if the Industrial Process Manager application is enabled.
- If the Industrial Process Manager is installed, then the site assigned to the OT device shows up in the **Site** field.
- If the Industrial Process Manager is enabled and there's only one entity that is associated with the OT device, then the **Equipment model entity** field is automatically populated.

Note: If multiple entities are associated with an device, the **Equipment model entity** field is left empty.

Result

The change request is created, and the users in the Assignment group, Assigned to, and Watch list fields are notified.

Create a change request from a remediation task

Create an Operational Technology (OT) change request from an OT remediation task. Creating a change request from a remediation task automatically populates the information in your change request record, such as the Site and the OT Device fields.

Before you begin

Roles required: sn_ot_change_write

Procedure

1. Navigate to All > **Industrial Workspace**.
2. Open the remediation task record that you want to create a change request from.
3. Select the **Create OT Change** button as shown in the following example.

The screenshot shows a remediation task record for 'VUL0010004'. The 'Remediation Progress' bar is at 0%. The 'Remediation Task Details' section includes fields like Number (VUL0010004), Risk rating (3 - Medium), and Created (2023-04-24 17:19:20). The 'Vulnerable items' table lists one item: 'VIT0010002' (Summary: A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka "Microsoft Graphics Components Remote Code Execution Vulnerability." This affects Windows 7, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft Excel Viewer, Microsoft PowerPoint Viewer, Windows Server 2019, Windows Server 2008 R2, Windows 10, Windows Server 2008). The 'Attachments' section indicates 'No Attachments Available'.

Note: If there's no active change model, the following error

Error creating Change Request: No active change model available. Please contact your OT Change admin

4. Select the OT change model that applies to your organization.

5. Select **Next**.

6. Complete the playbook as needed as your team works on the change request.

For more information about the Basic OT Change Model playbook, see [Basic OT Change Model playbook](#). For more information about the Advanced OT Change Model playbook, see [Advanced OT Change Model playbook](#).

The following fields are automatically populated depending on the conditions that you set.

- The **OT Device** field is auto-populated only if the Industrial Process Manager application is enabled.
- If the Industrial Process Manager is installed, then the site assigned to the OT device shows up in the **Site** field.
- If the Industrial Process Manager is enabled and there's only one entity that is associated with the OT device, then the **Equipment model entity** field is automatically populated.

i Note: If multiple entities are associated with an device, the **Equipment model entity** field is left empty.

Create a change request from an incident record

Create an Operational Technology (OT) change request from an OT incident record.

Creating a change request directly from an incident record helps automatically map data to the new change request from the incident record.

Before you begin

Role required: sn_ot_incident_write, sn_ot_incident_admin, or sn_ot_change_write

Procedure

- 1.** Navigate to **All > Industrial Workspace**.
- 2.** In the **OT Incidents** module list view, select one of the available lists.
- 3.** Select the incident record that you want to create an OT change request from.
- 4.** Select the **Create OT Change** button.
The **Select OT change** form opens.
- 5.** Select the change model applicable to your organization.
For more information, see [Select a change model to fulfill change requests](#).
- 6.** Select **Create OT Change record**.
- 7.** Fill in the playbook and related forms as needed.

For more information about the playbook and related forms, see [Basic OT Change Model playbook](#) and [Advanced OT Change Model playbook](#) depending on which OT change model you chose.

i Note: In the Details related list of the new change request, the following fields and related lists are automatically populated with the values from the related OT incident record:

- Site
- Equipment Model Entity
- OT Device (CI)
- Short Description
- Description
- Priority

i Note: A **Priority** field value from 1 through 4 is the same in the new change record. But a value of 5 in the incident record's **Priority** field is changed to 4 in the new change record.

Edit related devices and equipment model entities in a change record

Add or remove related Operational Technology (OT) devices and equipment model entities directly from an OT change record, which can help you keep track of the relationship between the change request and its effected items.

Before you begin

Role required: sn_ot_change_write or sn_ot_change_admin

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the **OT Change Requests** module list view, select one of the available lists.
3. Select the change record that you want to add or remove a related device or equipment model entity from.
4. To add a related OT device from the change record, do these actions:
 - a. Select the **Affected OT Devices** related list.
 - b. Select **Add**.
 - c. In the **Add OT Devices** window, select the check boxes next to the devices that you want to add.
 - d. Select **Add**.
The OT devices are now added to the change record under the Affected OT Devices related list.
5. To remove a related OT device from the change record, do these actions:
 - a. Select the Affected OT Devices related list.
 - b. Select the check boxes next to the devices that you want to remove.
 - c. Select the **Remove** button. A confirmation window appears asking if you want to proceed.
 - d. Select **Remove** in the window to continue.

The OT device or devices are removed from the change record and the Affected OT Devices related list.

- To add or remove an equipment model entity from a change record, repeat steps 4 and 5 but under the Impacted Equipment Model Entities related list.

Operational Technology change approval

The Operational Technology (OT) change approval lets reviewers approve your requested changes and suggest improvements as necessary.

Overview

An OT change approval with the Advanced OT Change Model enables approvers to review a change request, edit the request as necessary, and approve the change request.

Note: The change approval only applies to the Advanced OT Change Model. There's no change approval policy applied to the Basic OT Change Model.

Change approval requirements

Requirement	Description
Site level	Site or area where the change takes place.
Site approval group	Members assigned to an approval group that can review and approve change requests.
Role required	Approvers must have the sn_ot_change_read role.
Percentage of approvals	51% of the approval group has to approve the change for it to move forward.

OT change approval flow

The OT change approval flow is as follows.

- Create the change request.
- The flow is invoked based on the change model.
- The flow applies the change approval policy.
- Various decision records are evaluated.
- Matching approval definitions are executed.
- Add a list of site level approvers to the change record.

The Advanced OT Change Model contains a change approval policy. You can also create your own approval policy. For more information about how to create an approval policy, see [Create change approval policies](#).

Add an approver to review a change request

Add a group member, or approver, manually to your approval group to review your Operational Technology (OT) change request.

Before you begin

Role required: admin

Procedure

1. Navigate to **All > User Administration > Groups**.
2. From the Groups list, select the **OT Change Default Approvers** group.
3. Select the Group Members related list.
4. Select **Edit**.
5. In the Collection list, select the members that you want to add to the approval group.
6. Move the selected members to the OT Change Default Approvers list by using the middle arrows.
7. Select **Save**.

Result

New members have been added to your approval group. Now, the approval group can review your change request.

Managing change requests across sites

With the Change Writer role (sn_ot_change_write) of the Operational Technology Change Management application, you can view, create, or edit the change requests that belong to your site. You can also view the change requests from other sites so that you can implement similar changes at your site.

Overview

If you have the Change Write user role (sn_ot_change_write), you can do the following tasks:

- View and edit the Operational Technology (OT) change requests that are assigned to you or the change requests that belong to your site.
- Create OT change requests.
- View the OT change requests that belong to the other sites.

The following table describes the additional roles that you, as a user with the Change Write user role, need so that you can access the change requests for your site or any site.

Additional roles with the Change Write user role

Role	Permissions
sn_ot_change_write with the cmdb_ot_isa_editor role	Can create and edit change requests for your site.
sn_ot_change_write with cmdb_ot_isa_viewer role	Can create and edit change requests for your site.
sn_ot_change_write and cmdb_ot_isa_viewer_all	Can create and edit change requests for any site.
sn_ot_change_write with no site role	Can view change requests for any site.

Benefit of the Change Write user role

The main benefit of having the Change Write user role is that you have read-only visibility of changes across sites. Viewing other changes across sites can help you implement similar changes at your site.

Note: You can't edit the OT change requests for other sites. You can only edit the change requests that belong to your site.

Where to view or edit change requests

The following OT change request lists are available in the Lists module on the Industrial Workspace:

- Assigned to me: View and edit your assigned change records by navigating to **OT Change Requests > Assigned to me**.
- Belong to my sites: View and edit the change records that belong to your sites by navigating to **OT Change Requests > Belong to my sites**.
- View the existing change records at different sites by navigating to **OT Change Requests > All**.

Other OT change roles and permissions

The following table describes the other OT change roles and permissions that you, as a user with the Change Read user role, needs so that you can view the change requests for your site or any site.

Additional roles with the Change Read user role

Role	Permissions
sn_ot_change_read with the cmdb_ot_isa_editor role	Can view change requests for your site.
sn_ot_change_read with cmdb_ot_isa_viewer role	Can view change requests for your site.
sn_ot_change_read and cmdb_ot_isa_viewer_all	Can view change requests for any site.
sn_ot_change_read with no site role	Can view change requests for any site.

Visibility of change model records across sites

Depending on your Operational Technology (OT) change role and site role, you can view, create, or edit the change model record for your site or other sites.

OT Change roles and visibility to change model records

The following tables describe the roles and permissions for different OT change users to access change model records.

Permissions for users with the sn_ot_change_write role

Role	Permissions
sn_ot_change_write with cmdb_ot_isa_editor site role	Use a change model for their records.
sn_ot_change_write with cmdb_ot_isa_viewer site role	Use a change model for their records.
sn_ot_change_write with cmdb_ot_isa_viewer_all site role	Use a change model for their records.
sn_ot_change_write with no site role	No access to change models.

Permissions for users with the sn_ot_change_read role

Role	Permissions
sn_ot_change_read with cmdb_ot_isa_editor site role	No access to change models.
sn_ot_change_read with cmdb_ot_isa_viewer site role	No access to change models.
sn_ot_change_read with no site role	No access to change models.
sn_ot_change_read with cmdb_ot_isa_viewer_all site role	No access to change models.

Permissions for users with the sn_ot_change_manager role

Role	Permissions
sn_ot_change_manager with cmdb_ot_isa_editor site role	<ul style="list-style-type: none"> Create, edit, and delete change models for any site. Assign change models to any site. Remove change models from any site.
sn_ot_change_manager with cmdb_ot_isa_viewer site role	<ul style="list-style-type: none"> Create, edit, and delete change models for any site. Assign change models to any site. Remove change models from any site.
sn_ot_change_manager with no site role	Can't view or edit change models for any site. Can only view the base system change models that aren't associated with any site.

If you have the sn_ot_change_admin role, you can use the change models to create a change request for any site.

Change email notifications

Use email notifications to alert users when an Operational Technology (OT) change request or a change task is updated.

The notifications for OT change requests and change tasks are listed in the following tables.

OT change request email notifications

Name	When to send	Who receives it	What it contains
Change assigned to me	When the Assigned to field changes and is not empty.	User who's assigned the change	<p>Subject: <Change request #> notification</p> <p>Body:</p> <p>Short Description: <Short description></p> <p>Click here to view Change Request: <URL to the change request></p> <p>Site: <Site name></p> <p>OT Device: <OT device></p> <p>Equipment Model Entity: <Equipment model entity></p> <p>Description: <Description></p>
Change assigned to my group	When the Assignment group field changes and is not empty.	Assignment group	<p>Subject: <Change request #> has been assigned to group <assignment group></p> <p>Body:</p> <p>Short Description: <Short description></p> <p>Click here to view Change Request: <URL to the change request></p> <p>Site: <Site name></p> <p>OT Device: <OT device></p> <p>Equipment Model Entity: <Equipment model entity></p> <p>Description: <description></p>

OT change request email notifications (continued)

Name	When to send	Who receives it	What it contains
Change commented	When the change request is commented.	<ul style="list-style-type: none"> Requested By Watch list 	<p>Subject: <Change request #> comments added</p> <p>Body:</p> <p>Short description: <Short description></p> <p>Click here to view Change Request: <URL to the change request></p> <p>Comments: <Comments added to the change request></p>
Change worknoted	When a work note is added to the change request.	<ul style="list-style-type: none"> Work note list Assigned to Assignment group 	<p>Subject: <Change request #> work notes added</p> <p>Body:</p> <p>Short description: <Short description></p> <p>Click here to view Change Request: <URL to change request></p> <p>Work Notes: <Work notes added to change request></p>
Change approved	When the change request is approved.	<ul style="list-style-type: none"> Assigned to Assignment group 	<p>Subject: <Change request #> has been approved</p> <p>Body:</p> <p>Short Description: <Short description></p> <p>Click here to view <URL to change request></p> <p>Description: <Description></p>

OT change request email notifications (continued)

Name	When to send	Who receives it	What it contains
Change rejected	When the change request is rejected.	<ul style="list-style-type: none"> Assigned to Assignment group 	<p>Subject: <Change request #> has been rejected</p> <p>Body:</p> <p>Short Description: <Short description></p> <p>Click here to view <URL to change request></p> <p>Description: <Description></p>
Change on hold	When the change request is put on hold.	Requested By	<p>Subject: <Change request #> has been put on hold</p> <p>Body:</p> <p>Hello <user who created change request>,</p> <p>The <Change request #> you requested has been put on hold. The reason for the request being put on hold is: <Reason for change request being put on hold></p> <p>Click here to view your change request: <URL to change request></p>
Change off hold	When the change request is taken off hold.	Requested By	<p>Subject: <Change request #> has been taken off hold</p> <p>Body:</p> <p>Hello <user who created change request>,</p> <p>The <Change request #> you requested has been taken off hold and is in the</p>

OT change request email notifications (continued)

Name	When to send	Who receives it	What it contains
			<Updated state field> state. Click here to view your change request: <URL to change request>

OT change task email notifications

Name	When to send	Who receives it	What it contains
Change task assigned to me	When the Assigned to field changes and is not empty.	Person who is assigned the change task	Subject: <Change task #> notification -- <Short description> Body: Short Description: <Short description> Click here to view Change Task: <URL to change task> Site: <Site name> OT Device: <OT device> Equipment Model Entity: <Equipment model entity> Description: <Description>
Change task assigned to my group	When the Assignment group field changes and is not empty.	Assignment group	Subject: Subject: <Change task #> notification -- <Short description> Body: Short Description: <Short description> Click here to view Change Task: <URL to change task> Site: <Site name> OT Device: <OT device>

OT change task email notifications (continued)

Name	When to send	Who receives it	What it contains
			<p>Equipment Model Entity: <Equipment model entity></p> <p>Description: <Description></p>
Change task worknoted	When a work note is added to the change task.	<ul style="list-style-type: none"> Work note list Assigned to Assignment group 	<p>Subject: <Change task #> work notes added -- <Short description></p> <p>Body:</p> <p>Short description: <Short description></p> <p>Click here to view Change Task: <URL to change task></p> <p>Work Notes: <Work notes added to change task></p>

Operational Technology Change Management reference

Reference topics provide additional information about the Operational Technology Change Management application.

Related information

Find more information about the Operational Technology (OT) product view that is related to the ServiceNow® Common Service Data Model (CSDM), the Network Intrusion Detection System (NIDS), OT extension classes, and related applications.

Overview

The product view and the extension classes help you understand how Operational Technology Management works with the CSDM framework and the Configuration Management Database (CMDB) respectively.

[Operational Technology product view](#)

The Operational Technology product view helps you understand how Operational Technology key entities work with the CSDM framework.

[Operational Technology \(OT\) extension classes](#)

The Configuration Management Database (CMDB) updates classes for OT.

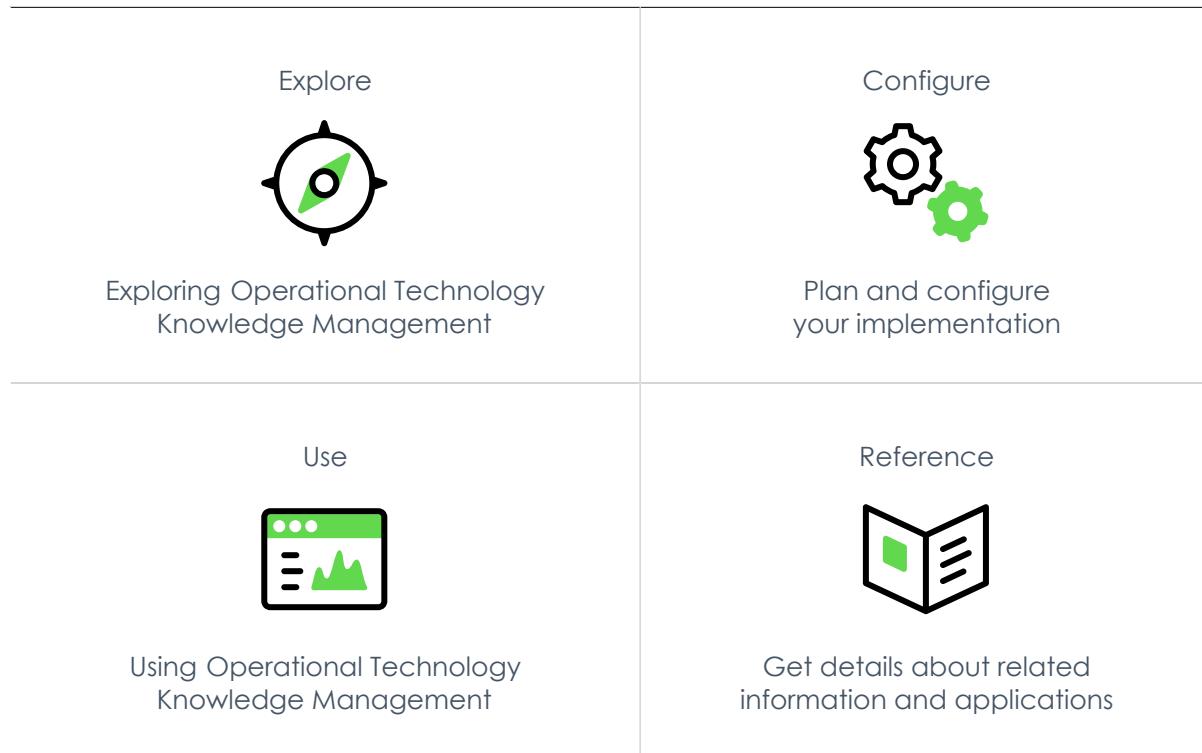
Related applications

[IT Service Management](#)

When integrated with Operational Technology Change Management, the ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Operational Technology Knowledge Management

ServiceNow® Operational Technology Knowledge Management can help you collect, organize, and share knowledge about your Operational Technology (OT) system, its devices, and the resolved incidents within your organization.



Exploring Operational Technology Knowledge Management

Operational Technology Knowledge Management helps you to capture information about your Operational Technology (OT) system in knowledge articles that are related to OT incidents. Your organization can then use these knowledge articles to help your users to access the right information and prevent miscommunication with your users.

Operational Technology Knowledge Management benefits

With Operational Technology Knowledge Management, you can use the following key features:

- Ability to use the existing Knowledge Management Now Platform capabilities with the Operational Technology Management solution.
- Ability to browse all knowledge base articles that are related to an OT incident and to create knowledge articles directly from an incident record.
- Ability to configure an OT knowledge base for knowledge managers and knowledge users.
- Ability to create knowledge articles in the Industrial Workspace.
- Ability to request approvals to publish, edit, retire, or delete a knowledge article.
- Ability to edit existing knowledge articles with updated information.

Configuring Operational Technology Knowledge Management

Configure Operational Technology Knowledge Management so that you can create the data foundation for the Operational Technology (OT) solution.

If you have the admin role, you can use Guided Setup to lead you through the setup of Operational Technology Knowledge Management. Guided Setup is a tool that assists with application configuration. It organizes the configuration activities into categories. These categories contain the information about the setup tasks, the steps to complete each task, and the links to the pages in your instance where you perform the configuration. The links to useful help content are also provided.

To access Guided Setup, navigate to **Industrial Workspace Admin > Guided Setup**.

The following table lists the Guided Setup tasks and their purposes for Operational Technology Knowledge Management.

Note: Operational Technology Knowledge Management is included with the Operational Technology Incident Management application. As long as you have the Operational Technology Incident Management application (version 2.0.2) installed and configured, you can configure Operational Technology Knowledge Management. No additional plugins are needed.

The following table shows the tasks that your users must complete for a successful setup and configuration.

Operational Technology Knowledge Management setup tasks

Task	Purpose
Assign Knowledge Management roles to Operational Technology Knowledge Management.	Assigns the roles to control the actions that are available for each user.
Create an OT knowledge base.	Configures an OT knowledge base to add managers and configure access.
Create user criteria to apply to an OT knowledge base.	Creates a user criteria record to determine the users who can read or contribute to an OT knowledge base.
Assign user criteria to an OT knowledge base.	Assigns the user criteria records to an OT knowledge base to control which users can create, read, write, and retire knowledge articles within the knowledge base.
Configure access to OT knowledge bases for unauthenticated users.	Reviews the OT knowledge bases that are accessible to unauthenticated users. Access is based on the user criteria and <code>glide.knowman.block_access_with_no_user_criteria</code> property settings.
Assign knowledge workflows to an OT knowledge base.	Assigns different knowledge workflows to each OT knowledge base for the publishing and retiring processes.
Review the Knowledge Management properties that are used for Operational Technology Knowledge Management.	Configures the look and functionalities of OT knowledge bases with the applicable Knowledge Management properties.

Assign roles to your Operational Technology Knowledge Management users

Assign Knowledge Management roles to your users so that you can control their access to the features, capabilities, and data for Operational Technology Knowledge Management.

Before you begin

Role required: admin

About this task

If you're assigned a Knowledge Management role, you can use the Operational Technology Knowledge Management capabilities.

- Note:** The user criteria determine the access to knowledge articles. For more information, see [Managing access to knowledge bases and knowledge articles](#).

For more information about the Knowledge Management roles applicable to Operational Technology Knowledge Management, see [Operational Technology Knowledge Management roles](#).

Procedure

Assign roles to users and groups by using the Now Platform user administration feature.

Task	User administration feature
Assign a role to a user	See User roles Edit user roles Assign user roles Assign roles to users
Assign a role to a group	See User roles Edit user roles Assign user roles Assign roles to users

Create an OT knowledge base

Create an Operational Technology (OT) knowledge base to provide a self-service platform for OT knowledge users to store, share, and manage content that is related to OT incidents.

Before you begin

Role required: admin

Procedure

1. Navigate to **Knowledge > Administration > Knowledge Bases**.
2. Select **New**.
3. On the knowledge base form, fill in the fields.
For a description of the field values, see [Knowledge base form](#).
4. Right click the form header and select **Save**.
5. In the related list section, view or configure the items in the following table that are related to the OT knowledge base.

Name	Description
Knowledge	List of knowledge articles that are stored in this knowledge base.
Can Read	List of user criteria that grants read access and enables a user who matches the

Name	Description
	criteria to read articles in the OT knowledge base.
Can Contribute	List of user criteria that grants contributor access and enables users who match the criteria to create and modify the articles in the OT knowledge base.
Article Templates	<p>If you've activated the Knowledge Management Advanced (com.snc.knowledge_advanced) plugin, the Article Templates related list is displayed.</p> <p>If article templates are in the related list, the articles in that knowledge base can only be created by using one of the article templates listed.</p> <p>If the Article Templates related list is empty, articles can be created by using any article template.</p> <p>Map article templates to the knowledge base by selecting Edit.</p> <p>i Note: Admins, knowledge admins, and knowledge managers can edit the article templates for the knowledge base.</p>
Knowledge categories	<p>List of knowledge categories that are associated with the OT knowledge base.</p> <p>i Note: If the category is marked as inactive, then you can't associate articles to the category. However, it doesn't affect the existing articles of that category.</p>

6. Select **Submit**.

Create the user criteria for an OT knowledge base

Create a user criteria record to determine the users who can read or contribute to an Operational Technology (OT) knowledge base.

Before you begin

Role required: user_criteria_admin

i Note: To create a user criteria record from the Knowledge module, you must have the user_criteria_admin role in addition to the knowledge role. For more information about access, see [Managing access to knowledge bases and knowledge articles](#).

About this task

Use the user criteria in Knowledge Management to determine whether certain users can access OT knowledge bases and knowledge articles. After you create a user criteria record, you can assign it to an OT knowledge base to control who can read and contribute to a knowledge base and its articles. You can further assign the user criteria at an article level to control who can read it.

Procedure

1. Navigate to **All > Knowledge > Administration > User Criteria**.
2. Select **New**.
3. On the form, fill in the fields.

User Criteria form

Field	Description
Name	Unique name of the user criteria.
Users	Users who must match the user criteria.
Groups	Groups that must match the user criteria.
Roles	Roles to match the user criteria. <p>Note:</p> <ul style="list-style-type: none"> ◦ Because the evaluation of a role is cached in the session, any change in the role requires you to log in again. ◦ User criteria are not applicable for elevated privilege roles.
Advanced	Option to display or hide the advanced option that includes the Script field on the User Criteria form.
Script	Script to define any additional user criteria that returns true or false. This field is available when the Advanced option is selected on the User Criteria form. <p>Note:</p> <ul style="list-style-type: none"> ◦ A script is evaluated in the scope that the user criteria are created in. ◦ The evaluation of a script is cached in the session, so any change in the evaluation requires you to log in again. If a scripted user criterion is defined for a knowledge base, the user access to the knowledge bases is evaluated after every session. If the script results in changes after a session cache is built, the result takes effect in the next session. ◦ Don't use <code>gs.getUser()</code> or other session APIs because they cause conflicts when used in diagnostic tools. Use the predefined <code>user_id</code> variable available in the script to get the user ID of the user being used to evaluate the script. ◦ Scripts are evaluated dynamically. Therefore, including scripts in a user criteria can impact the performance of your system.
Active	Option to activate or deactivate the user criteria.

Field	Description
Companies	Companies that the user record must match.
Locations	Locations that the user record must match.
Departments	Departments that the user record must match.
Match All	<p>Option to determine whether all elements from each populated user criteria field must match. If selected, only the users who match all user criteria are given access. If cleared, the user must meet one or more of the set user criteria to be given access.</p> <p>By default, this check box is cleared so that any condition met provides a match.</p> <p>For example, consider a user criteria record for the following conditions:</p> <ul style="list-style-type: none"> ◦ Locations A or B ◦ Company C or D <p>With Match All selected, only the users who meet all of these conditions are matched. For example, a user with a location A and a company C.</p> <p>If Match All isn't selected, users who meet any of these conditions are matched. For example, a user with a location B.</p> <p>Note: If you select Match All, ensure that you don't create contradictory conditions that can never be met. For example, if all users in location A work for company G, the conditions in this example can never be met.</p>

4. Select **Submit**.

What to do next

Now you can assign the user criteria to an OT knowledge base. For more information, see [Assign the user criteria to an OT knowledge base](#).

Assign the user criteria to an OT knowledge base

Assign the user criteria records to an Operational Technology (OT) knowledge base to control which users can create, read, write, and retire knowledge articles within the knowledge base.

Before you begin

Role required: knowledge_manager, knowledge_admin, or admin

About this task

You can assign user criteria to an OT knowledge base to control read or contribute access.

Procedure

1. Navigate to **All > Knowledge > Administration > Knowledge Bases**.
2. Select the OT knowledge base record that you want to manage.
3. Add the user criteria to the OT knowledge base.

- a. Depending on the user criteria that you want to set, select one or more of the related lists.

Related list	Description
Can Read	Users can read knowledge articles in the knowledge base.
Cannot Read	Users can't read knowledge articles in the knowledge base.
Can Contribute	Users can create, modify, and retire knowledge articles in a knowledge base. Contribute access to a knowledge base also provides read access to all articles in the knowledge base.
Cannot Contribute	Users can't create, modify, retire, or read knowledge articles in the knowledge base.

- b. In the selected related list, add the required user criteria.

- As a user with the admin role, add a new user criteria record by selecting **New**, specifying the required fields, and selecting **Submit**.
- As a user with the knowledge_manager, knowledge_admin, or admin role, add an existing user criteria record by selecting **Edit**, moving the required user criteria from the Collection column to the Knowledge column, and selecting **Save**.

4. On the knowledge base form, select **Update**.

Review access to OT knowledge bases for unauthenticated users

Review the Operational Technology (OT) knowledge bases that are accessible to unauthenticated users by using the user criteria and `glide.knowman.block_access_with_no_user_criteria` property settings.

Before you begin

Role required: knowledge_admin or admin

About this task

If you want to restrict unauthenticated users for a knowledge base, you can use the user criteria or the `glide.knowman.block_access_with_no_user_criteria` property settings.

Procedure

1. Navigate to **All > Knowledge > Administration > Knowledge Bases**.
2. Review the OT knowledge bases that are accessible to unauthenticated users.
3. Optional: To restrict unauthenticated users for a knowledge base by using the user criteria, select the knowledge base record and update its user criteria.
For more information about creating the user criteria, see [Create the user criteria for an OT knowledge base](#). For more information about assigning the user criteria, see [Assign the user criteria to an OT knowledge base](#).
4. Optional: Restrict unauthenticated users for a knowledge base by using the `glide.knowman.block_access_with_no_user_criteria` property settings.

- a. Navigate to **All > Knowledge > Administration > Properties**.
- b. Set the `glide.knowman.block_access_with_no_user_criteria` property settings to true.
- c. Select **Save**.

Assigning knowledge workflows to an OT knowledge base

You can assign different Knowledge Management workflows to each Operational Technology (OT) knowledge base for the publishing and retiring processes.

Overview

You can use the default Knowledge Management workflows in the following table for Operational Technology Knowledge Management and apply them to OT knowledge bases.

Note: For the workflows that require approval, you can configure which users can approve or reject by editing the `getApprovers()` function in the `KBWorkflow` script include.

Default Knowledge Management workflows

Workflow	Description
Knowledge - Approval Publish	<p>Requests approval from a manager of the knowledge base. Articles in approval have a state of In Review before moving to a Published state after approval. If they're set to publish later, they're moved to a Scheduled state. If the manager rejects the request, the workflow is canceled and the article remains in the Draft state.</p> <p>If the ownership groups option is enabled, email notifications with a link to the article are sent to the ownership group members for approval.</p> <p>If the ownership groups option isn't enabled, email notifications with a link to the article are sent to the knowledge base managers for approval.</p> <p>A notification is also sent to the authors or the revisers of the articles to inform them that their article has been approved or rejected.</p> <p>To turn on the approval email notifications, set the <code>glide.knowman.enable_approval_notification</code> property to <code>true</code>.</p> <p>Note: Only the active user receives the notifications.</p>
Knowledge - Approval Retire	Requests approval from a manager of the knowledge base before moving the article

Default Knowledge Management workflows (continued)

Workflow	Description
	<p>to the retired state. If any manager rejects the request, the workflow is canceled and the article remains in the Published state.</p> <p>If the ownership groups option is enabled, email notifications with a link to the article are sent to the ownership group members for approval.</p> <p>If the ownership groups option isn't enabled, email notifications with a link to the article are sent to the knowledge base managers for approval.</p>
Knowledge - Instant Publish	Immediately publishes a draft article without requiring an approval, or publishes on the scheduled publish date if set to publish later.
Knowledge - Instant Retire	Immediately retires a published article without requiring an approval.
Knowledge - Publish Knowledge	Subflow that moves the knowledge article to the Published state. You can use this subflow when defining your own workflow.
Knowledge - Retire Knowledge	Subflow that moves the knowledge article to the Retired state. You can use this subflow when defining your own workflow.

Email notifications for approval workflows

You can send email notifications for approval workflows.

- Notify approvers about the knowledge articles submitted for their approvals.
- Notify authors about the approval status of their knowledge articles

To send email notifications for approval workflows, enable the **Send notification to approvers and authors in article approval workflow** property (`glide.knowman.enable_approval_notification`). Beginning with the New York release, the property is enabled by default. Existing customers on release versions prior to the New York release can enable this property to send email notifications. Disable any custom notifications for article approvals before enabling this property. If the `glide.knowman.enable_approval_notification` property isn't available, an administrator can create the property and set its value to true. For more information, see [Knowledge Management properties](#).

Reviewing the Knowledge Management property for an Operational Technology knowledge base

As an administrator, you can configure the look and functionalities of Operational Technology (OT) knowledge bases with the Knowledge Management properties.

You can access the Knowledge Management properties by navigating to **All > Knowledge > Administration > Properties**.

Use the property that is listed in the following table to control which roles can flag incomplete or inaccurate articles in knowledge bases.

Glide.knowman.show_flag.roles property

Property	Description
List of roles (comma-separated) that can flag incomplete/inaccurate articles (<code>glide.knowman.show_flag.roles</code>)	<p>Enter the role names exactly as they appear in User Administration > Roles. If both the Show article rating section and Show "Flag Article" option properties are selected, the users with the roles listed in this property see the flag article option in the article view.</p> <p>All roles listed in this property must also be listed in the List of roles that can see an article's rating section property.</p>

For more information about the other available Knowledge Management properties, see [Knowledge Management properties](#).

Using Operational Technology Knowledge Management

After you complete all the required set-up tasks for Operational Technology Knowledge Management, you can begin managing knowledge articles that are related to Operational Technology (OT) incidents.

Overview

By using#Operational Technology Knowledge Management, you can create, edit, and retire knowledge articles depending on the needs of your team. When used with the Operational Technology Incident Management application, you can browse articles that are related to an incident and create articles from an incident.

The following examples show how to apply#Operational Technology Knowledge Management to your team:

- An OT engineer with several years of experience wants to capture their OT device knowledge in one place for guide workers and junior technicians.
- Front-line workers and technicians responsible for production process operations have noticed an issue on the factory floor and need a knowledge article that explains remediation.

Knowledge articles

Knowledge articles provide information about workplace updates, self-help, troubleshooting steps, and other information that your OT team must access. For example, you can create the following knowledge articles for the following cases:

- A standard operating procedure template used throughout your organization.
- Lessons learned during an incident.
- An image that annotates the different production materials.

You can view the knowledge articles in the Industrial Workspace in the following ways:

- Under the Knowledge module in the Industrial Workspace list view.
- In the Agent Assist window when you open an OT incident.
- Using the global search feature in the Industrial Workspace header.

Under the Knowledge module in the Industrial Workspace list view, you can view knowledge articles in the following lists:

Note: You must be assigned the knowledge role to see these list modules in the Industrial Workspace.

Your unpublished articles

The articles you've created that aren't yet published in the OT knowledge base.

Your published articles

The articles you've created that are published to the OT knowledge base.

All articles

All articles that are available in the OT knowledge base.

Create a knowledge article from an OT incident record

Create a knowledge article to record and save information that is related to an Operational Technology (OT) incident and its resolution.

Before you begin

Role required: sn_ot_incident_write

Note: You also need the **Can contribute** access to at least one knowledge base. For more information, see [Create an OT knowledge base](#).

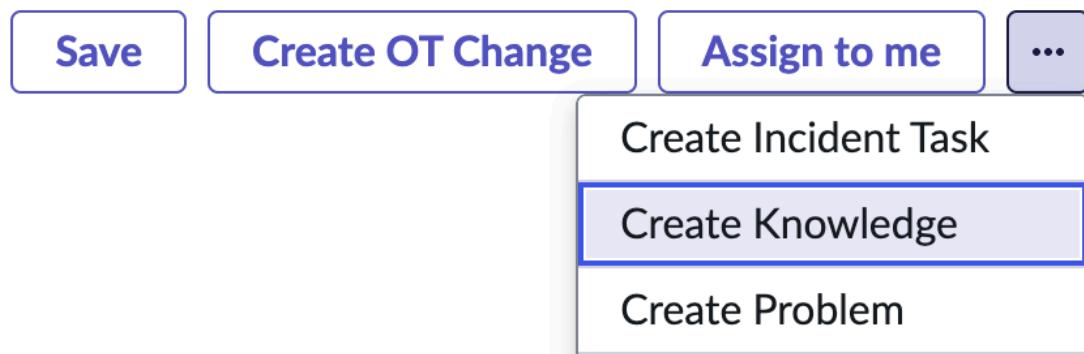
About this task

Creating a knowledge article directly from an incident record helps to make sure that the knowledge article is linked to the correct incident for contextual information. The knowledge article can also help your team resolve similar incidents in the future when they include the correct procedures, challenges, and solutions.

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the list view under the OT Incident module, open one of the available lists.
3. Select the OT incident record that you want to create a knowledge article for.
4. Select the **More actions** button  to expand the menu.

5. Select **Create**



Knowledge.

i Note: You must set the incident record's state to **Resolved** to see the **Create Knowledge** button.

6. On the form, fill in the fields.

Knowledge article form

Field	Description
Knowledge base	Knowledge base that the knowledge article should be included in. i Note: If you configured the OT knowledge base's visibility correctly, OT users can find the knowledge base in this reference list.
Category	Classification of the knowledge article.
Short description	Brief description of the incident resolution that is used as the knowledge article title.
Article body	Content of the knowledge article that describes any procedures, challenges, and solutions for the incident.
Valid to	Date that the knowledge article is valid until.

7. Select **Save**.

The knowledge article is saved as a draft and attached to the parent OT incident.

8. Select **Publish**.

Result

The knowledge article is now published in your OT knowledge base. To view the knowledge article, open the Attached Knowledge related list in the incident record.

i Note: If you set the **Publish workflow** field in your OT knowledge base to **Knowledge - Approval Publish**, the article must be approved before being published.

Create a knowledge article in Industrial Workspace

Create a knowledge article in Industrial Workspace to help cater an article's contents to the needs and solutions not directly related to an Operational Technology (OT) incident.

Before you begin

Role required: knowledge

Note: You also need the **Can contribute** access to at least one knowledge base. For more information, see [Create an OT knowledge base](#).

Procedure

1. Navigate to **All > Industrial Workspace**.

2. In the list view under the Knowledge module, open one of the available lists.

3. Select



4. On the form, fill in the fields.

Knowledge article form

Field	Description
Knowledge base	Knowledge base that the knowledge article should be included in. Note: If you configured the OT knowledge base's visibility correctly, OT users can find the knowledge base in this reference list.
Category	Classification of the knowledge article.
Short description	Brief description of the incident resolution that is used as the knowledge article title.
Article body	Content of the knowledge article that describes any procedures, challenges, and solutions for the incident.
Valid to	Date that the knowledge article is valid until.

5. Select **Save**.

The knowledge article is saved as a draft and attached to the parent OT incident.

6. Select **Publish**.

Result

The knowledge article is now published in your OT knowledge base.

Note: If you set the **Publish workflow** field in your OT knowledge base to **Knowledge - Approval Publish**, the article must be approved before being published.

Report a knowledge gap from an OT incident record

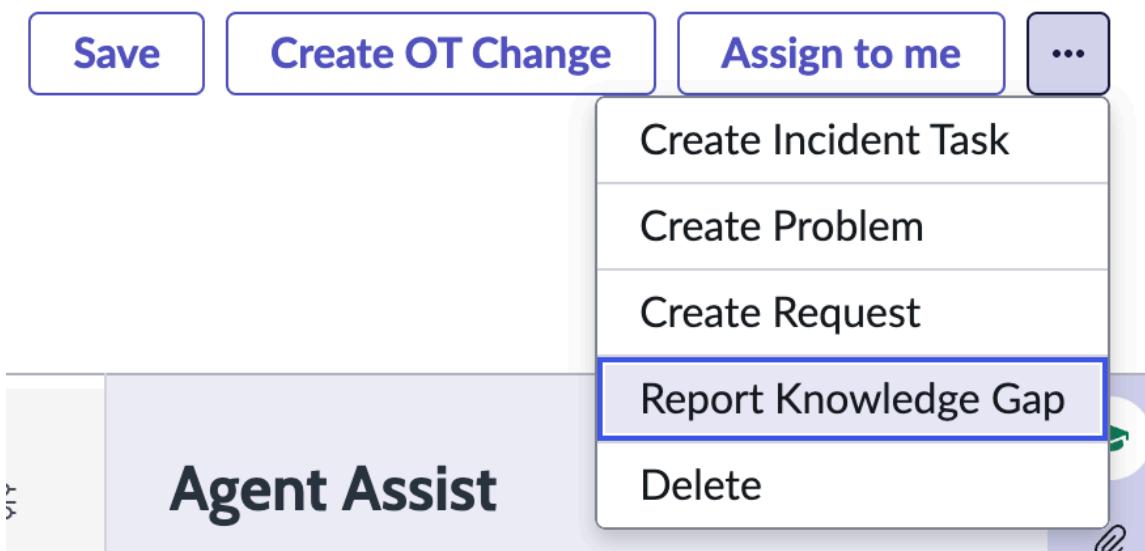
Report a knowledge gap from an Operational Technology (OT) incident if you can't find relevant knowledge articles about the incident.

Before you begin

Role required: sn_ot_incident_read

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the list view under the OT Incident module, open one of the available lists.
3. Select the incident record that you want to report a knowledge gap for.
4. Select the **More actions** button  to expand the menu.
5. Select **Report Knowledge**



6. On the form, fill in the **Description** field with a summary of the knowledge gap.

Note: The **Topic** field automatically fills with the name of the incident record. If needed, you can change this field.

7. Select **Submit**.

Result

The knowledge gap is reported and a feedback task is created.

What to do next

You can view the feedback task under the Knowledge Gaps related list in the incident record.

To assign feedback tasks to the correct user or user group, see [Assign feedback tasks](#).

Approve requests to publish or retire a knowledge article

Approve requests to publish or retire a knowledge article to help ensure that the knowledge base is up to date.

Before you begin

Role required: knowledge_manager

About this task

If you're assigned as the manager of an OT knowledge base receive, you can receive approval requests for the publishing and retiring of articles that belongs to the knowledge base.

Procedure

1. Open the email notification regarding the approval request.
2. Select the link in the email to open the request.
3. Approve or reject the request.
4. Optional: If rejected, leave a comment explaining why the article request was rejected.

Result

The user who created the approval request is notified via email.

Assign feedback tasks

Assign feedback tasks to a user to help make sure that the feedback task is addressed and the related knowledge article is updated.

Before you begin

Role required: knowledge_manager

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the list view under the Knowledge module, open the Unassigned OT Knowledge Gaps list.
3. Select the feedback task that you want to assign to a user or assignment group.
4. In the **Assigned to** field, add the user that you want to assign the feedback task to.
5. Select **Save**.

Result

The assigned user can now view the feedback task in the My Feedback Tasks list under the Knowledge module list view.

To view other assigned feedback tasks, select the Assigned Feedback Tasks list under the Knowledge module list view in the Industrial Workspace.

To view the unassigned OT knowledge gaps, select the Unassigned OT Knowledge Gaps list under the Knowledge module list view in the Industrial Workspace.

Find information in the related knowledge articles for an OT incident

Find information in the related knowledge articles that are attached to an Operational Technology (OT) incident record for any previous resolutions that may be applicable.

Before you begin

Role required: sn_ot_incident_read

- Note:** You must have the sn_ot_incident_read role and read access to the knowledge base that contains the articles that match the context of this incident.

Procedure

1. Navigate to **All > Industrial Workspace**.
2. In the list view under the OT Incident module, open an available list.
3. Select the incident record that you want to view.
4. In the incident record, select the **Agent assist** button  to open the Agent Assist window if it's not already opened.
5. To view the full knowledge article, select the **More actions** button .
6. Select **Full View**.
7. Optional: To attach the knowledge article to the open incident record, select **Attach** in the Agent Assist window.
8. Optional: To flag the knowledge article, select **Flag** in the Agent Assist window.
9. Optional: To mark the knowledge article as helpful, select the **More actions** button  and choose **Helpful**.

Operational Technology Knowledge Management reference

Reference topics provide additional information about the Operational Technology Knowledge Management application.

Operational Technology Knowledge Management roles

You can assign Knowledge Management roles to your Operational Technology Knowledge Management users.

The following table lists the Knowledge Management roles that you can assign to your users so that they can access Operational Technology Knowledge Management capabilities.

Knowledge Management roles applicable to Operational Technology Knowledge Management

Role	Description
knowledge	<p>The knowledge role can contribute to the default knowledge base and access the Knowledge application menu. The knowledge role is a fulfiller role and not a requester role.</p> <p>Note: Requesters can view, comment, and give feedback to the knowledge articles. However, a requester can't create or edit articles.</p>
knowledge_manager	<p>The knowledge manager can perform administrative functions for the knowledge bases that they manage, such as defining the categories, pinning the important articles, and approving the changes to the articles. Users selected as managers of a knowledge base receive this role automatically.</p>

Knowledge Management roles applicable to Operational Technology Knowledge Management (continued)

Role	Description
	<p>i Note: The knowledge role comes as a subordinate role.</p>
knowledge_admin	<p>The knowledge administrator can perform all the administrative tasks that are associated with maintaining the Knowledge Management system.</p> <p>i Note:</p> <ul style="list-style-type: none"> A user selected as a knowledge admin can make changes to all the knowledge bases except the scoped knowledge base. The knowledge role comes as a subordinate role.

Knowledge base form

When creating a new knowledge base, fill out the following form fields.

Knowledge base form fields

Field	Description
Title	Unique name for the OT knowledge base.
Article Validity	Number of default days that the articles are valid for after the date that they're created.
Icon	Image that provides a visual reference to describe the OT knowledge base. The image is displayed next to all articles from this knowledge base in the article search results page.
Disable commenting	Option to disable commenting. If selected, users can't comment on articles in the OT knowledge base.
Disable suggesting	Option to disable edit suggestions. If selected, users can't suggest edits to articles in the OT knowledge base.
Disable category editing	Option to disable the editing of OT knowledge categories. If selected, only OT knowledge managers can add or edit the knowledge categories for the OT knowledge base.

Knowledge base form fields (continued)

Field	Description
Disable rating	Option to disable the rating for articles. If selected, users can't rate the article in the OT knowledge base.
Disable mark as helpful	Option to disable the mark as helpful. If selected, the user can't mark any article as helpful in the OT knowledge base.
Enable blocks	Option to enable the knowledge blocks feature. If selected, you can create knowledge blocks to add to knowledge articles within the OT knowledge base.
Checklist	Checklist to evaluate the quality of articles in the OT knowledge base.
Application	Application scope of the OT knowledge base.
Owner	User responsible for the OT knowledge base. A knowledge base owner can assign other roles to the knowledge base.
Managers	Users who perform administrative functions on the OT knowledge base.
Publish workflow	Workflow for publishing the articles in the knowledge base: <ul style="list-style-type: none"> Knowledge - Instant Publish: Publishes articles in the knowledge base without requiring an approval. Knowledge - Approval Publish: Requests an approval from the manager of the knowledge base before moving the articles to the published state.
Retire workflow	Workflow for retiring the articles in the OT knowledge base: <ul style="list-style-type: none"> Knowledge - Instant Retire: Retires the articles in the knowledge base without requiring an approval. Knowledge - Approval Retire: Requests an approval from the manager of the knowledge base before moving the articles to the retired state.
Active	Option to indicate that the OT knowledge base is active. If not selected, only users with the admin role or knowledge administrators can create, search for, or view its articles.
Description	

Knowledge base form fields (continued)

Field	Description
Set default knowledge field values	Default configuration settings for the OT knowledge base.
Related products	List of products that are related to the OT knowledge base content.

Operational Technology Knowledge Management related information

Find more information about the Operational Technology (OT) product view that is related to the ServiceNow Common Service Data Model (CSDM), the Network Intrusion Detection System (NIDS), OT extension classes, and related applications.

Overview

The product view and the extension classes help you understand how Operational Technology Management works with the CSDM framework and the Configuration Management Database (CMDB) respectively.

[Operational Technology product view](#)

The Operational Technology product view helps you understand how Operational Technology key entities work with the CSDM framework.

[Operational Technology \(OT\) extension classes](#)

The CMDB updates classes for OT.

Related applications

[Knowledge Management](#)

The Knowledge Management application enables the sharing of information in knowledge bases. These knowledge bases contain articles that provide users with information such as self-help, troubleshooting, and task resolution.

[Operational Technology Incident Management](#)

The Operational Technology Incident Management application enables manufacturers to manage OT device incidents from the time the incident is opened to when it's complete.

[IT Service Management](#)

When integrated with Operational Technology Knowledge Management, the ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Domain separation and Operational Technology

Domain separation is supported for the Operational Technology application. 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: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see [Application support for domain separation](#).

Overview

The Operational Technology application inherits the domain separation features of the dependency applications. As each application can have its own domain separation relationship, there is no one specific support level to associate with the Operational Technology application. To learn more, see [Domain separation and Flow Designer](#).

Related topics

[Domain separation for service providers](#)