

Before you begin

Role required: admin

Procedure

1. Navigate to **All > System UI > View Rules**.
2. To only view the OT View Rules, apply the following filter:
[Name] [contains] [OT]
3. For the OT View Rule that you want to edit, select the **Read-only** value in the **Protection policy** column.
4. Change the **Protection policy** column value to **--None--**.

Result

Changing the **Protection policy** column value from **Read-only** to **--None--** allows users assigned the **admin** role to edit the OT View Rule.

Related information

Find more information about the Network Intrusion Detection System (NIDS) extension class, OT extension classes, and related applications.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

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 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.

**Operational Technology Discovery**

You can use the Operational Technology Native Discovery solution to amplify the visibility of devices in your OT environment. You can also use the IT Discovery for Operational Technology (OT) Networks function to discover IT class OT devices.

Get started

Use these links to explore and learn more about the Operational Technology Native Discovery components or the IT Discovery for Operational Technology Networks.

Explore



Operational Technology
Native Discovery components

IT Discovery for Operational
Technology (OT) Networks

Troubleshoot and get help

If you have any errors or difficulties while using the Operational Technology Discovery applications, [Contact Customer Service and Support](#). 

Operational Technology Native Discovery components

The ServiceNow® Discovery for Operational Technology (OT) Native components provide a solution that gives you visibility of your OT devices and imports your device data into ServiceNow using the Service Graph Connector for ServiceNow OT Discovery. Using the OT components, that is, the Discovery Console for OT, Discovery Sensor for OT, and OT Discovery Collector, you can monitor and query your devices within the OT environment.

Operational Technology Native Discovery components

Review and install the Service Graph Connector for ServiceNow OT Discovery then install the OT Discovery components. The first component to start with is the Discovery Console for Operational Technology (OT).

Note: For more information, see [Service Graph Connector for ServiceNow Operational Technology \(OT\) Discovery](#).

Use the links in the Related Topics section to explore the Operational Technology Native Discovery components.

Deploy Operational Technology Discovery

Consider deployment options for your Operational Technology Discovery components.

Where to start

You can use the links in the Related Topics section to consider and learn more about deploying the Operational Technology Discovery components.

Architectural considerations

This document intends to describe the ServiceNow Operational Technology Discovery architecture and covers how discovery components find, identify, and inventory devices in an Operational Technology environment.

Operational Technology Discovery software architecture

Today's industrial environments are made up of hundreds — sometimes thousands — of connected devices: programmable logic controllers, remote terminal units, human-machine interfaces, protection relays, and more. Tracking all of them — what they are, where they sit in your network, and whether they behave as expected — is a foundational challenge of operational technology.

The following describes the software architecture underlying the ServiceNow Operational Technology Discovery platform.

How Discovery works

At its core, Operational Technology Discovery actively reaches out to devices on your network using the same protocol language those devices already speak. Each device receives a query in its native protocol and responds with identifying information. A Modbus device gets a Modbus query. An EtherNet/IP device gets an EtherNet/IP query. This approach avoids aggressive network scanning that can disrupt sensitive industrial equipment.

The result is an updated inventory of your OT environment, visible through a single interface and integrated directly into your broader IT service management platform.

Note: The user sets the protocol parameters for the query from the Discovery Console for OT.

Active Discovery approach

Before exploring how the discovery components work in detail, it helps to understand the Operational Technology Discovery uses an active discovery approach.

The **Active** discovery initiates communication directly with devices using their native industrial protocol language — sending the same kinds of queries an engineering workstation or HMI would send to a PLC. These queries are indistinguishable from normal operations. Devices can't distinguish these queries from regular engineering traffic, making properly implemented active discovery safe for operational networks.

Active discovery is easier to setup and start because it can require a Console and a single Sensor or Collector rather than a distributed set of SPAN ports and collection devices.

The key advantage of active discovery is coverage. Because it reaches out to devices rather than waiting for them to communicate, it can detect silent and dormant assets that passive monitoring would never see. It also retrieves granular details — firmware versions, serial numbers, configurations — that may never appear in normal network traffic.

The Discovery components

The architecture is built around three components that work together. It is important to understand each component's distinct role and responsibilities.

The Discovery Console for OT is the interface you use to configure discovery, define the areas of your network you want to scan, and view the results. You can place more than one Console in your network.

- The Console is your starting point. It is where you define your industrial sites, configure the network zones and sites you want to discover, and set up the queries that drive the process. After discovery is running, the Console is also where you view results — seeing your OT environment take shape as devices are identified and cataloged.
- In terms of network placement, the Console typically, but not necessarily, sits in an IT/OT DMZ or a dedicated secure management zone. It doesn't perform discovery itself, but it configures the Sensor and serves as the central point of visibility across your entire deployment.

The Discovery Sensor for OT does the discovery work. Deployed as software on a virtual machine or physical server, the Sensor reaches out to devices in your network, identifies them, and builds your device inventory. It does this actively — on a schedule you configure. You can place Sensors throughout your network.

- The Sensor does the active discovery. Deployed as software on a virtual machine or bare metal system, it executes the queries configured in the Console. It builds your device inventory from the responses it receives. When the Sensor queries a device, it uses that device's native industrial protocol — Modbus, DNP3, EtherNet/IP, and others. This keeps the interaction safe for the network. You can select the protocol for the query in the Console.
- However, industrial environments are often deeply segmented by design — and the Collector addresses this.

The OT Discovery Collector extends the Sensor's reach into parts of your network that the Sensor can't access directly. In large or highly segmented industrial environments, a single Sensor may not have network visibility into every zone. Collectors are lightweight components deployed within those zones to bridge the gap. You can also use more than one of these components in your OT environment.

- The Collector is a (small) application that can be installed on existing systems (for example, HMIs) to extend discovery.
- Combined with the Sensor, it offers flexible deployment options to assist with maximum coverage of the OT network.

The Discovery workflow

It is easier to understand how the three components work together when you follow a discovery job from start to finish. The following covers that process — from building a query in the Console through to a fully populated device inventory in the ServiceNow instance.

Step 1: The network is built with Discovery in mind

Before any discovery runs, the Consoles, Sensors, and Collectors are deployed at positions in the network that reflects the user's OT environment. There are no fixed rules about how many OT components are needed to deploy or exactly where to place them. This depends on your OT network.

Sensors and Collectors are deployed to cover the network. They can be deployed on bare-metal hardware or on a Virtual Machine, depending on what suits each part of the network. The Console, however, is recommended to run on a Virtual Machine. Discovery can return photographic data alongside standard device attributes. A Linux distribution should be installed on the same VM before the Console is installed.

Step 2: Build a query in the Console.

Discovery begins when you create a query in the Console, where you define exactly what you want to discover and how. Query parameters include:

- **Protocols:** Which industrial protocols to use when communicating with devices, such as Modbus, DNP3, or EtherNet/IP.
- **Brands:** Filtering discovery toward specific device manufacturers if needed.
- **Ports:** Which network ports to include in the query.
- **Assets:** Which devices or ranges of devices to target.
- **Sites:** You can create or discover sites.
- **Query type:** Simplified and advanced query types such as the OPC-UA type, which captures photographic and visual data from devices rather than relying solely on protocol-based communication.

You can also select specific Sensors and Collectors the query should use. Because Sensors and Collectors are deployed at known positions in the network, you can pick specific components

by name — choosing the Sensor inside Line #1, for example, because you know that's where the devices you want to discover are located. Alternatively, you can let the query use the appropriate components based on where they are positioned in the network.

Step 3: The query runs through the selected components.

Once configured and launched, the query drives everything. Each Sensor and Collector executes the query within its part of the network, reaching out to devices using the protocols and parameters the user defined. A Sensor handles discovery in the zones it can directly access. A Collector does the same in the deeper or more restricted zones where it has been positioned.

Because both Sensors and Collectors are independently deployed and selectable, a single query can span multiple zones simultaneously. The Sensor handles one part of the network and the Collector handles another, all driven by the same query configuration.

Step 4: Results upload to ServiceNow.

As devices respond, their details are collected and returned to the Console. These include device type, vendor, model, firmware version, network address, zone, Purdue level, and where applicable, photographic data. From the Console, the data is uploaded to the ServiceNow instance.

i Note: It should be noted that depending on your network structure, there are additional OT components used to reach the ServiceNow instance, if needed. For further information on OT Discovery connections, see the [OT Discovery deployment scenarios](#) or the [Service Graph Connector for ServiceNow OT Discovery Guided Setup](#).

Within the ServiceNow instance, discovered devices are mapped to configuration items predefined in the CMDB. These configuration items are based on industry and operational device types, reflecting the OT world your team works in every day. They can be edited and adjusted to fit the data retrieved, giving your team flexibility to tailor the inventory to your environment.

The result is an accurate, up-to-date inventory of your OT environment — built through the discovery components your company has positioned in the network. It is visible through a single interface and integrated directly to ServiceNow without manual surveys or spreadsheets.

Wrapping up

Operational Technology Discovery is built on the principle that visibility should not come at the cost of safety. By deploying the Console, Sensor, and Collector at deliberate positions within your network — and querying devices in a way that is safe for operational environments — the system adapts to your environment rather than requiring you to adapt your environment to it. Whether you're managing a single compact site or a large enterprise with dozens of segmented zones, the architecture scales accordingly. The result is a current, accurate inventory of your OT environment, fully integrated into ServiceNow and built without disrupting the operational processes your network supports.

Before deploying OT Discovery

To discover assets in your OT environment, the Operational Technology Discovery solution provides the ServiceNow platform, the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector.

Before you deploy

Consider these questions before planning your Operational Technology Discovery deployment. This list is not exhaustive.

- Are you looking at OT devices or IT devices in the OT network?
- Have you planned the Site location?
- What is the network layout and architecture of the Site location? Is it a flat or segmented layout?
 - The best way to start is to place a Discovery Sensor for OT in a location that includes many of the devices to be queried.
 - Next, place additional Sensors in areas of the network that might have segmentation or other barriers, such as a NATed environment or segmented silos.
- Are there any network zones in place? Identify any NATed networks or copy-paste networks (sites with identical IP ranges).

i Note: When Sensors can reach the same zoned location or when assets are dual-homed, carefully document the zoned Sensor configuration to avoid creating duplicate asset records.

- What communication pathways exist within the site?
- If Sensors are deployed in each Network (NW) zone, can they communicate with the assets in the OT network?
- Do any other devices have to be installed?
- Where does the Discovery Console for OT get installed?
- Can one Console be used for multiple sites or does the deployment require one Console per site?
- Are there communication paths between the Sensors and the Console?
- Does the MID Server exist in DMZ?
- Is there a communication path between the Console and the MID Server?
- Are there any other tools (IDS or Discovery tools) in the OT environment?

Adding capabilities over time

With OT Discovery, you can add layers of capabilities over time such as:

- Deploying the Discovery Console for OT and Discovery Sensor for OT in a central location with access to multiple sites.
- Deploying the Discovery Sensor for OT at individual sites, with additional Sensors deployed as needed for policy enforcement or non-IP-enabled asset monitoring.

Adding locations over time

On a site-by-site level, you can add locations over time, such as deploying the Discovery Console for OT and the Discovery Sensor for OT at a pilot site. For more information, see the [Sites page](#).

OT Discovery System Resources

You can review the OT Discovery component resources before setting up your OT network.

OT Discovery components required resources

The requirements in this section are a generalization. Consider factors such as segmentation level, communication pathways, network traffic, redundancy, and environmental conditions. Also account for physical constraints when determining network requirements. The following tables provide resource estimates for each OT Discovery component. Review your system requirements beyond these minimums.

Discovery Console for OT System requirements

Component	Minimum System Requirements
Discovery Console for OT	• 16 GB RAM • 100 GB Hard drive • 2 CPUs

For additional requirements for the Console, see [Requirements for Discovery Console for OT installation](#) and [Install the Discovery Console for Operational Technology \(OT\)](#).

Discovery Sensor for OT System requirements

Component	Minimum System Requirements
Discovery Sensor for OT	• 2 GB RAM* • 100 GB Hard drive • 2 CPUs • 2 virtual NIC cards *8 GB of RAM is recommended for all queries.

For additional requirements for the Sensor, see [Configure the Discovery Sensor for OT](#).

Note: The Collector can be installed and run on either a Windows OS or a Linux OS.

OT Discovery Collector minimum system requirements

Component Operating System	Minimum System Requirements
Windows	The OT Discovery Collector installation is compatible with Windows 10 or Windows 11 systems. The required Windows (10 or 11) environment for the OT Discovery Collector is x86_64. ARM or Apple Silicon devices aren't supported. See Install the OT Discovery Collector on a Windows system.
Linux	See Install OT Discovery Collector on a Linux system for specific information.

OT Discovery communications

This section describes how the OT Discovery components should be connected so they can communicate with each other.

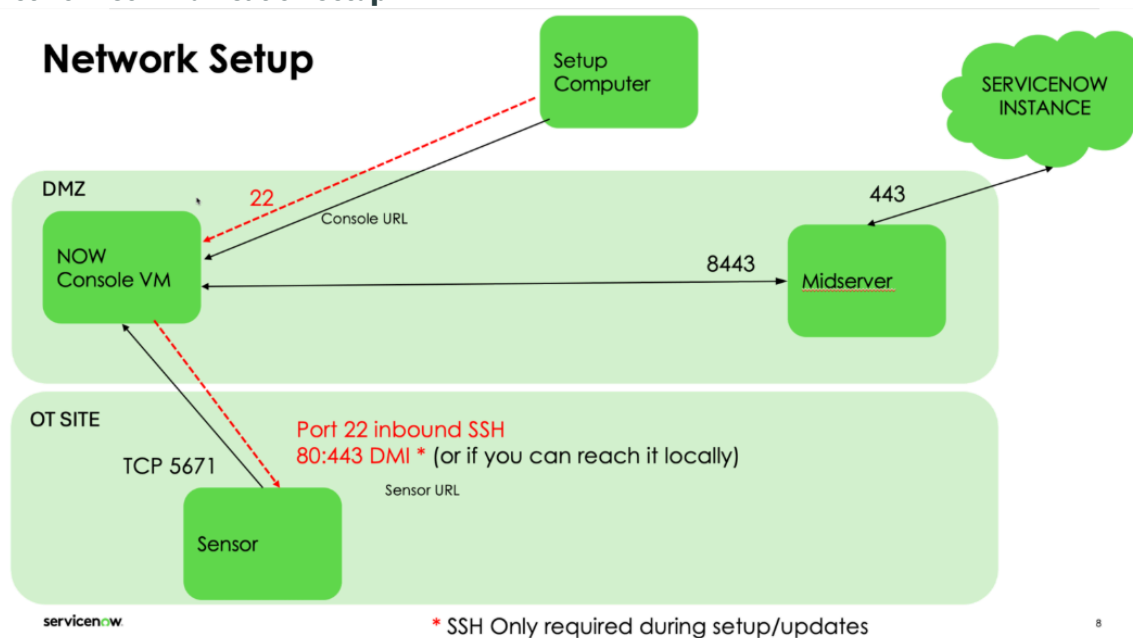
Component communications

When determining the environment architecture for your deployment, consider how the following OT Discovery components interact.

- MID Server-to-ServiceNow instance:
 - The MID Server needs to communicate with the ServiceNow instance to push the information from Discovery Console for OT.
- Note:** If the Discovery Console for OT can reach the internet, the MID Server might not be needed in your OT configuration.

 - This configuration and deployment is the same as with any other MID Server.
 - The Service Graph Connector (SGC) needs to communicate with the MID Server, the Console, and the ServiceNow instance.
- Console-to-MID Server communication:
 - Deploy a separate MID Server for each network or network segment.
 - Configure firewall rules to enable communication across networks or network segment boundaries.
 - The Console needs to communicate with the Sensors, the Collectors, the MID Server, the SGC, and your ServiceNow instance.

Network communication setup



- Sensor-to-Console communication:
 - Deploy a separate Console for each network, network segment, or system.
 - Configure firewall rules to enable communication across networks or network segment boundaries.

- The Discovery Sensor for OT needs to communicate with OT assets and with the Discovery Console for OT.
- Discovery Sensor for OT data is pushed to the ServiceNow instance by the Service Graph Connector.
- Sensor-to-asset communication:
 - Deploy a separate Sensor for each network, network segment, or system.
 - Configure firewall rules to enable communication across network, network segment, or system boundaries.
- Discovery OT Collector-to-Console communication:
 - Discovery OT Collector needs to communicate with the Console.
 - The Collector communicates with the Console and with your system's assets.

Network port map

The following table describes how to set up network ports.

Network port map

Source	Destination Port	Direction	Destination	Required/Optional	Description
Management Console	8443 (HTTPS) inbound	Bi <->	Workstation	Required	Console web interface
Management Console	5671 (AMQP) inbound	Uni <-	Sensor	Required	Communications from Sensors to Console
Management Console	123 (NTP) inbound	Uni <-	Time Server / Esxi Host	Optional	Clock synchronization, Not needed if time server or hypervisor will provide time.
Management Console	8443 API	Uni <-	MID Server	Required	Import data from Management Console via the APIs.
Management Console	22 (SSH) inbound	<-	Host Setup Computer	Optional (setup)	Additional support during deployment
Sensor	5671 (AMQP) outbound	Uni <-	Management Console	Required	Communications from Sensors to Console
Sensor	443 (HTTP) inbound	<-	Host Setup Computer	Required	Additional support during deployment

Network port map (continued)

Source	Destination Port	Direction	Destination	Required/Optional	Description
Sensor	22 (SSH) inbound	<-	Host Setup Computer	Required	Additional support during deployment
MID Server	443	Bi <->	NOW instance / Web	Required	Communications from the MID Server to the NOW fabric internet facing.

OT Discovery deployment scenarios

Deployment scenarios for OT Discovery vary based on a network's architecture. Use these scenarios to help determine how to deploy the OT Discovery components in your OT environment.

Note: The OT Discovery Collector can be deployed to the same locations as the Discovery Sensor for OT.

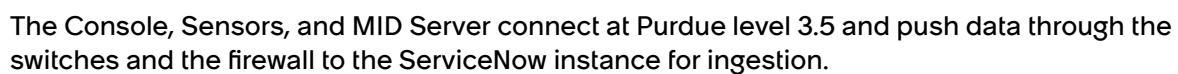
General recommendations

General recommendations and guidance are listed in each scenario in these sections. Not all networks are the same. The requirements in this section are a generalization for the scenario. Consider factors such as segmentation level, communication pathways, network traffic, redundancy, and environmental conditions. For resource recommendations for the OT Discovery components see, [OT Discovery System Resources](#).

Flat network architecture across multiple sites

A flat network architecture is a network design that has all available Discovery Console for OT, Discovery Sensor for OT, and OT Discovery Collector connected to a single network, where the Sensors and Collectors can communicate with each other directly.

You can have one or more sites that communicate with each other.

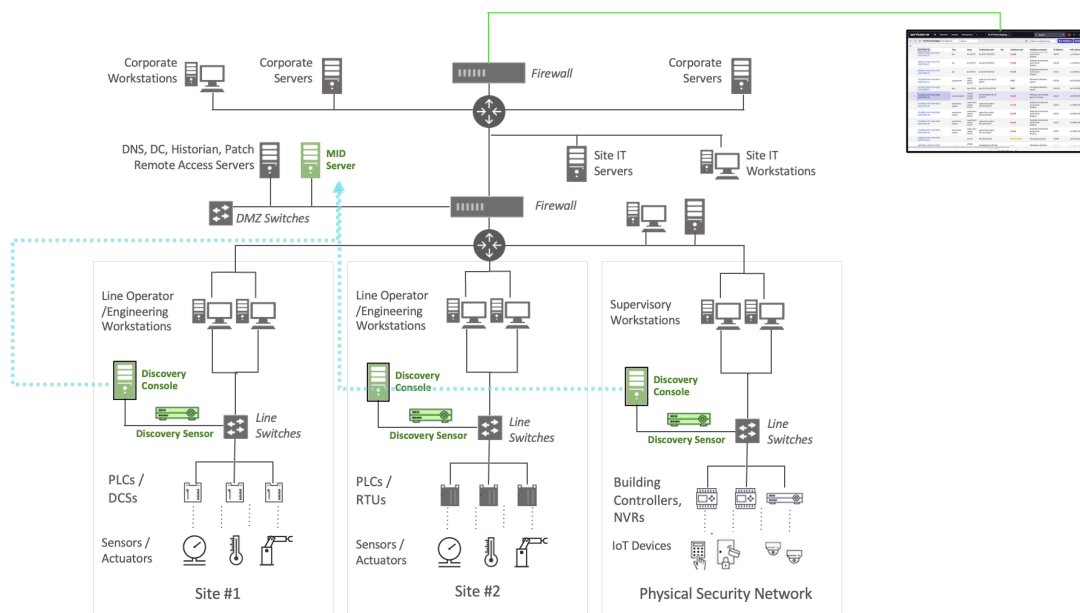


The following are the components in a flat network.

- Discovery Console for OT and Discovery Sensor for OT.
- A localized appliance or VM that serves as the command-and-control interface for asset discovery and communication in its respective segment. This appliance or VM manages credentials, protocol handlers, and initiates querying operations locally. In such a scenario, a typical deployment means that one Console covers multiple sites.
- Deploy the Console at a layer where the MID Server can connect to the Console and the ServiceNow instance.
- Deploy Sensors based on the desired speed of the discovery. In a truly flat network, a Discovery Sensor for OT can reach all the OT assets in that network. More Sensors in the network can help improve the speed of discovery.

A segmented site architecture is a network design that has the network split into multiple segments. Each segment contains its own Discovery Console for OT and multiples of the Discovery Sensor for OT and the OT Discovery Collector. There is no communication between sites. Each of the segments could be considered a flat network.

Segmented sites



In this OT environment, the network is segmented into three distinct zones for operational clarity, security, and control:

- Site 1 Operational Technology segment
- Site 2 Operational Technology segment
- Physical Security Network segment

Each segment contains its own isolated infrastructure to reduce risk and increase visibility in its respective domain. Components in each segment:

- Discovery Console for OT or VM that serves as the command-and-control interface for asset discovery and communication in its respective segment. It manages credentials, protocol handlers, and initiates scanning operations locally.
- Discovery Sensor for OT is deployed in each segment. The Sensor performs active discovery, collects network traffic, and queries for known protocols (for example, Modbus, DNP3, BACnet). It reports findings to its segment's Console.

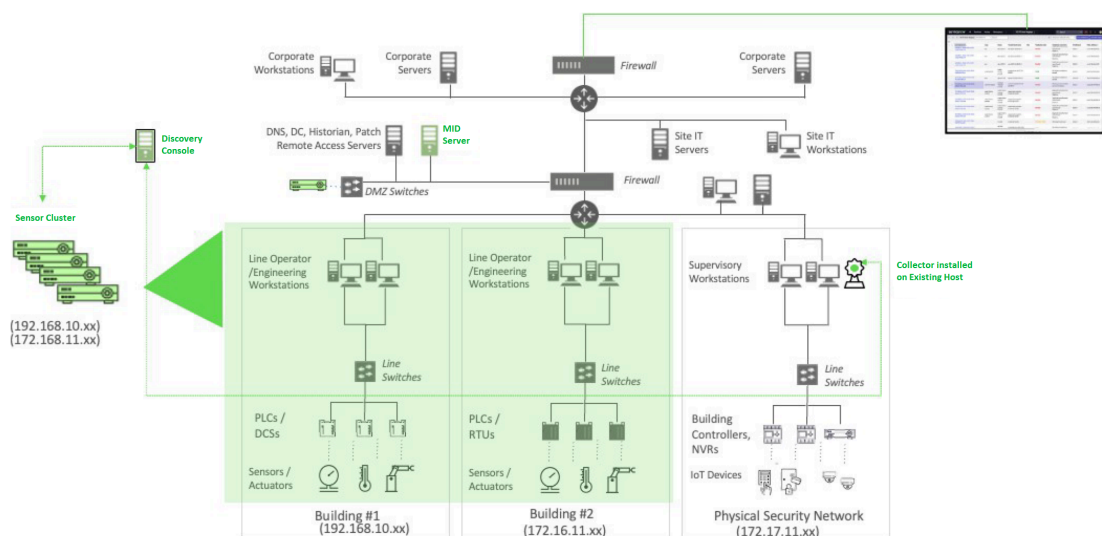
The Consoles and Sensors are deployed in their respective network zones and don't have direct outbound access to the internet.

Micro-segmented site with multiple networks

A segmented site architecture with multiple networks is a network design that has more than one network split into multiple segments. Each segment contains multiple network segments and its own Discovery Console for OT and Discovery Sensor for OT.

- Make sure the Sensors and Collectors have a communication pathway to the Console.
- Deploy Sensors in each segment where the Sensor can perform active discovery in the segment and collect network traffic and can scan or query for known protocols (for example, Modbus, DNP3, BACnet). It reports findings to its segment's Console.
- If you use an existing host to do the discovery in the network such as Human Machine Interface (HMI) or Engineering Workstation (EWS), you can install the OT Discovery Collector to perform discovery.

Segmented site with multiple networks



Discovery Console for Operational Technology (OT)

Use the Discovery Console for OT component to discover, monitor, and query devices in your Operational Technology environment.

Get started

Use the links in the Related Topics section to explore, configure, and learn more about the ServiceNow Discovery Console for OT.

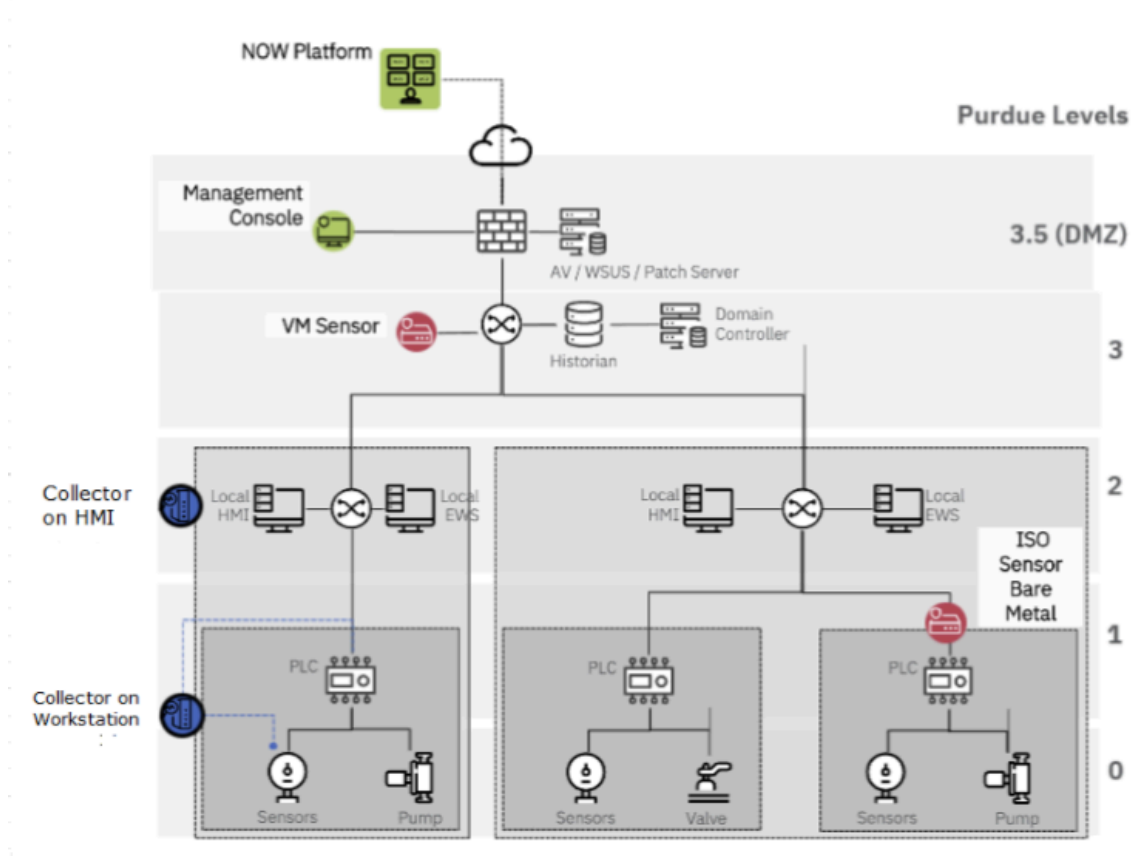
Explore the Discovery Console for Operational Technology (OT)

The Discovery Console for OT provides you with enhanced features to discover your assets in the OT environment.

Discovery Console for OT Overview

The Discovery Console for OT provides complete operational technology visibility across your entire OT environment. This awareness starts at the Human Machine Interface (HMI Purdue Reference Model Levels 2 and 3) and goes down to the field devices (Level 0) through the Discovery Console for OT Network and Sensors. From the Discovery Console for OT you can enable and configure device management capabilities. The Discovery Console for OT and Discovery Sensor for OT work together to create a comprehensive device inventory that you can monitor and manage from a single interface.

Purdue levels



Discovery Console for OT uses and benefits

Some of the uses and benefits of the Discovery Console for OT are as follows.

- **Uses**
 - You can use the Console as a configuration manager for your OT devices.
 - Configure schedules, manage sites, networks zone, configure discovery settings, review the asset data, and provide access to additional users.
 - You can manage and monitor several Discovery Sensor for OT and OT Discovery Collector components.
- **Benefits**
 - Acts as a single source of truth for all OT Devices discovered in the Sites.
 - The Console manages OT assets and provides visibility to OT operators.\

Accessing the Discovery Console for OT

Access to the Discovery Console for OT requires these steps:

- **Note:** Before you can use the Console, you must have a license. Request a Console license from your ServiceNow account representative.

1. Have an active ServiceNow® instance.
2. Go to the ServiceNow Store, acquire and install the Service Graph Connector for ServiceNow OT Discovery, and navigate to the SGC Guided Setup page.

3. The first step of the Guided Setup is to select the link to the **Download & Deploy** for the OT Discovery components.
4. From there, download the installation packages for the Console, Sensor, and Collector, as desired.

Note: It's recommended that you install the components in this order: Console, then Sensor, and then Collector.

5. The Console installer packages must be installed on a virtual machine with a Linux distributed OS.

Use the Discovery Console for OT interactive configuration wizard

The Discovery Console for OT provides an interactive configuration wizard that steps you through setting up your Console, Sensor, Collector, assets, queries, and sites.

Before you begin

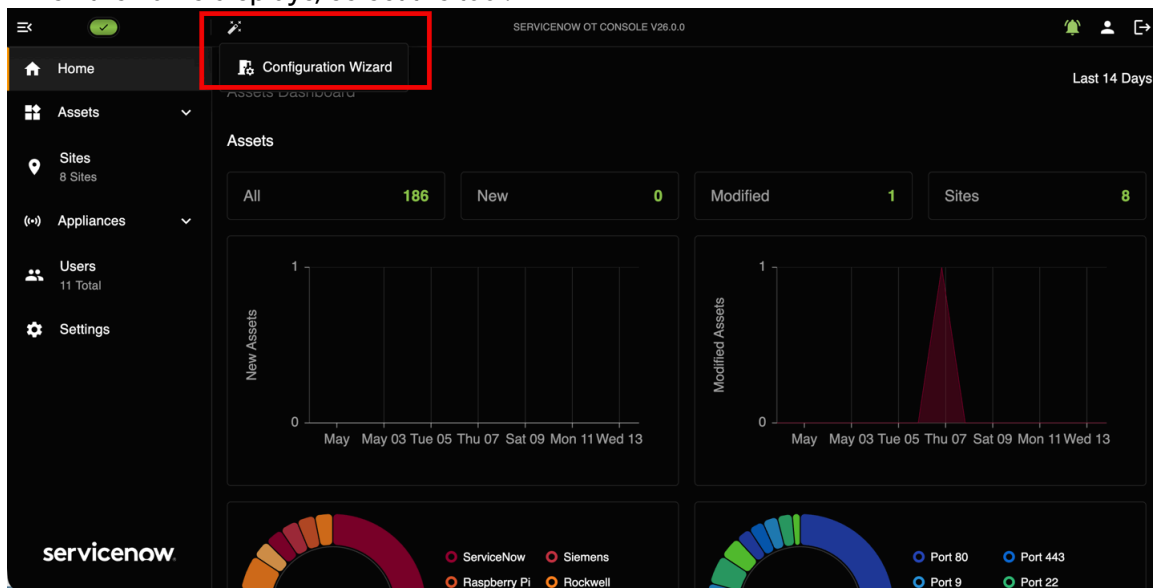
Role required: admin

About this task

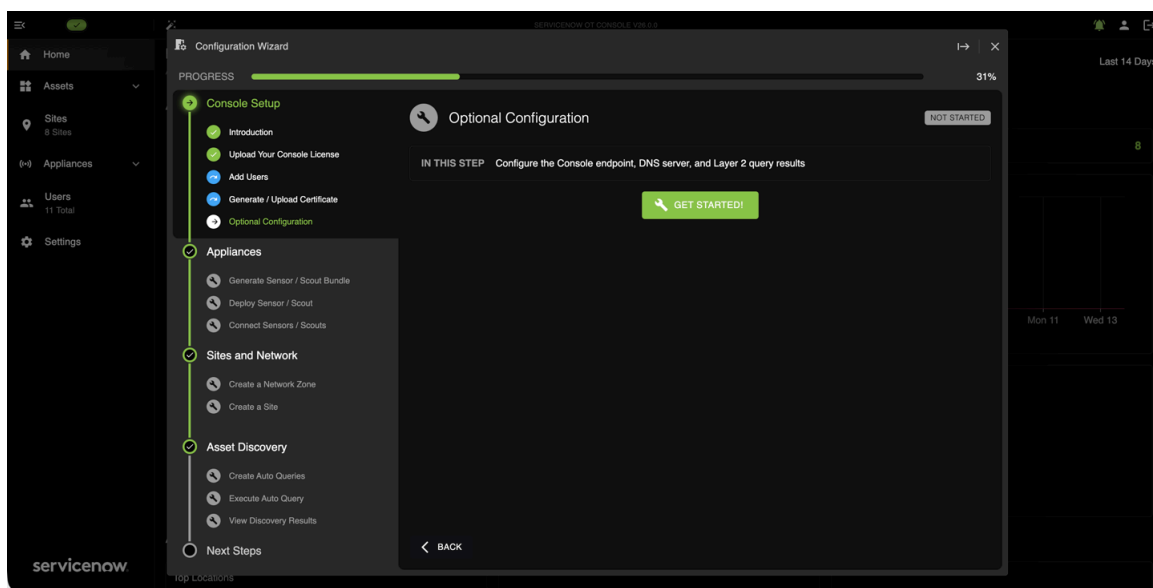
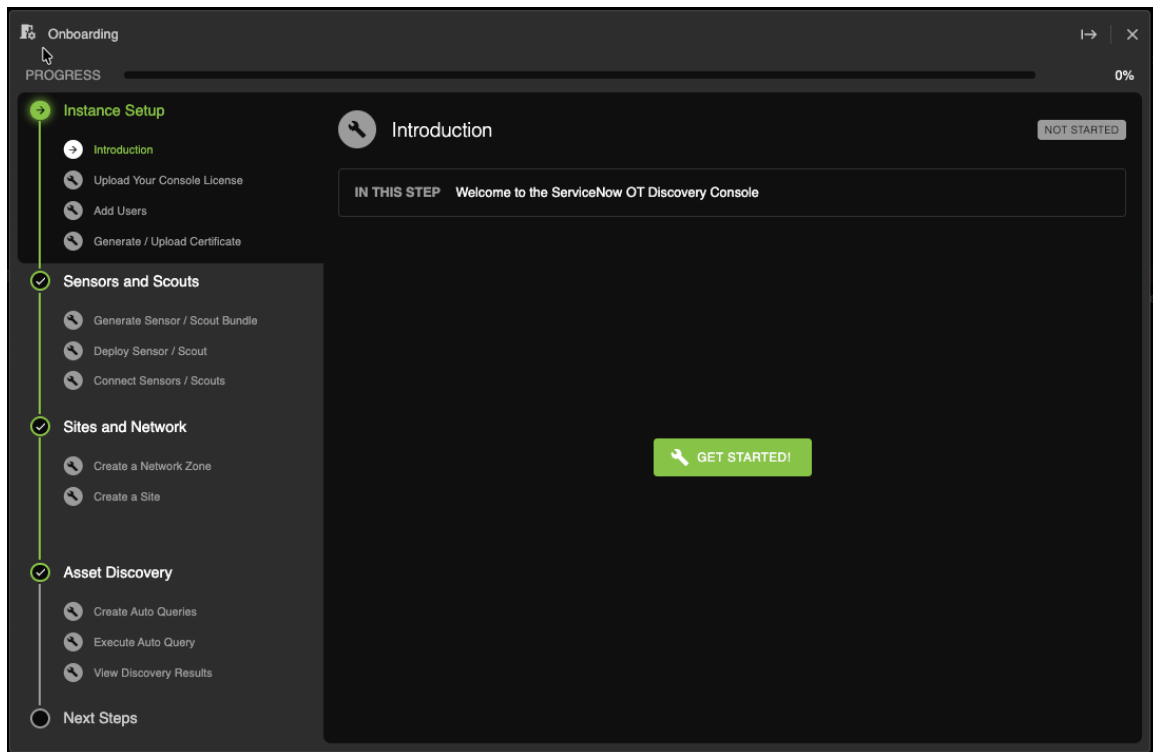
After you have installed and setup the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector on your system, the Console's interactive configuration wizard is available for use. The wizard steps through the initial tasks for using the Console, setting up Sensors and Collectors, and gives you an overall introduction to using the OT components.

Procedure

1. On the Console **Home** page, select the wand at the top of the page (Tools).
2. When the name displays, select the tool.



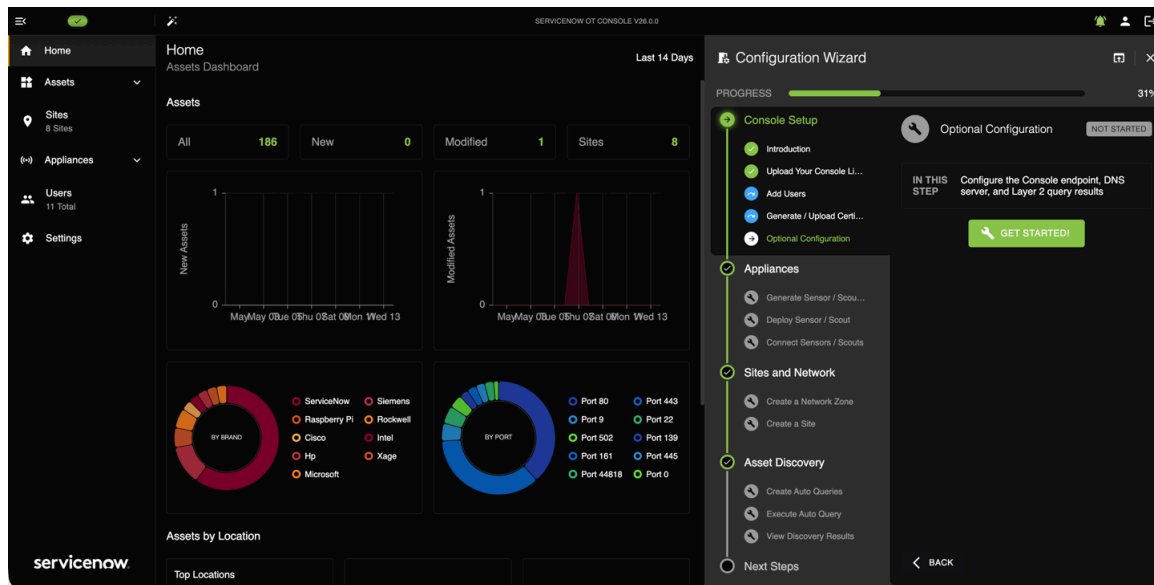
3. The configuration wizard opens in the Console.



4. You can collapse the wizard to the right side of the Console screen by selecting the  icon in the top, right corner of your screen.

Move the wizard to the right (collapse) to improve Console visibility.

To expand and center the wizard on the screen, select the  icon.



5. The wizard steps you through tasks such as configuring your Console, connecting the Sensor and Collector, creating a site, and creating Auto Queries.
6. Just follow the steps in the wizard and when you complete each one, mark them as **Done**.
7. The wizard provides a **Skip** button so you can skip any of the optional steps.
8. You can open the configuration wizard on any Console page by selecting the **Tool** wand.

Configure the Discovery Console for OT

This section is an overview of the steps for installing the Discovery Console for OT.

Note: During the installation of the non-containerized version of Discovery Console for OT, you must have access the internet to download and install dependent third-party packages such as MongoDB and RabbitMQ. The Console installation automatically installs these packages as long as there's an internet connection. After installation of the third-party packages, the internet connection is unnecessary.

Workflow

In your instance, navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup page and select Get Started. In the top section, select the Download & Deploy OT Discovery link. The Download & Deploy OT Discovery page opens. Select **Configure** and the Downloads page opens. Download the OT component packages.

Note: The required dependency version has been changed to .NET 10 from .NET 8

Review the steps in the installation process listed in the Installation Workflow table.

Discovery Console for OT Installation Workflow

Task	Description
Install virtual machine	You can use any type 1 or type 2 hypervisor. For example: - VMware - Hyper-V - Azure

Discovery Console for OT Installation Workflow (continued)

	• AWS • Google Cloud • Proxmox
Install Linux distribution on the VM.	Install Linux or install a compatible Linux distribution such as: • RedHat Enterprise Linux (RHEL) 8.x, 9x, and 10x • Rocky 8.x, 9x, and 10x • Debian 12 and 13 • Ubuntu 22.04 and 24.04
Hardware requirements	• RAM: 16 GB (Recommended) • Hard Disk drive: 100 GB • CPUs: 2 For more information, see OT Discovery System Resources.
Connection	Confirm that you have access to the ServiceNow instance.
Installation packages	As previously stated, from the Downloads page, download the Discovery Console for OT, Discovery Sensor for OT, and the OT Discovery Collector packages.
Containerized packages	For closed network systems, you can download and install containerized packages for the Console and the Collector. Select the Collector package that is compatible to your machine's OS. For more information, see Air-gapped networks and OT Discovery installation .
Begin the install for the Discovery Console for OT	Install the Discovery Console for OT before you install the Discovery Sensor for OT. Install the OT Discovery Collector last.
Move the package into the VM	Move the Console installer package into the VM.
Extract the installer	From the Console package, extract the ConsoleInstaller .ZIP file.
Run the installation script	Execute <code>./console-init.sh</code>. This script confirms all the required components are installed. Note: If you're using the traditional console package (that is, non-containerized package) you need access to internet to download dependent third-party packages such as MongoDB and RabbitMQ.
Accessing the web console	To access the web console UI, open the browser and navigate to <code>https://<IP address of the console VM>:8443</code> .

Discovery Console for OT Installation Workflow (continued)

Register initial user	Before you can log in to the Console for the first time, you must register as a user. In the log in window: 1. Enter your username and an email. 2. Create your own password or generate a random password. 3. Copy and save this password. 4. Enter the password. 5. Select the check box, I acknowledge I saved my password. 6. Select Enter. Note: Make sure to save the password, to avoid getting locked out of the system. For more information, see Log on to the Discovery Console for OT.
EULA Agreement	Next, the EULA appears on the screen. Accept the EULA by checking the box next to Agree.
Generate a new certificate	After the Console is installed, generate a new Console certificate. For more information, see Generate a certificate.

Note: Once installation is complete, and you log in to the Console, you can choose to use the interactive configuration wizard. The wizard guides you to upload your Console license. It also takes you through the getting started with the system, such as: creating a Site, creating a Network Zone, and building your initial Auto Query. For more information, see [Use the Discovery Console for OT interactive configuration wizard](#).

Air-gapped networks and OT Discovery installation

This section explains the options for air-gapped and non-air-gapped network, installation of Discovery for OT components, and accessing data from scans and queries.

Non-air-gapped networks

During the installation of the Discovery Console for OT, you must have access to the internet to download and install dependent third-party packages such as MongoDB and RabbitMQ. The Console installation automatically installs these packages as long as there's an internet connection. After installation of the third-party packages, the internet connection is unnecessary.

When using the installation for a non-air-gapped network, the Discovery Console for OT not only needs access to dependent third-party packages, but it also needs to communicate with the Sensors, the Collectors, the MID Server, the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery, and your ServiceNow instance.

For these specific steps see the documentation on configuring the individual OT Discovery components. Start with [Configure the Discovery Console for OT](#).

Air-gapped networks

If you plan to install the Discovery Console for OT on an air-gapped network, additional steps are needed to move your queried data from your OT components and environment to your ServiceNow instance.

One way to work around this type of network is to first install the OT Discovery component packages on your network. The challenge is then how to get the data from your network to the Mid Server so that it is uploaded to the ServiceNow instance. To do this:

1. Run queries within your closed network with the OT Discovery components to generate the desired data.
2. Download the physical data files from the Console to a physical, portable storage device (USB drive).
3. Then manually move these files to the MID Server.
4. On the MID Server, create a folder for your files.
5. Copy the physical files to this folder on the MID Server.
6. The MID Server uploads your data to your ServiceNow instance.

What to do next

For more information, see [Install containerized OT Discovery packages](#).

Install containerized OT Discovery packages

Install the OT Discovery containerized packages on your network.

Before you begin

Role required: admin

About this task

To help meet the air-gapped challenge, ServiceNow provides containerized versions of the Discovery Console for OT and the OT Discovery Collector. The Discovery Sensor for OT package has everything it needs and can be installed as is to an air-gapped network. The following steps cover installation of the containerized Console and Collector packages.

Procedure

1. On your ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page.
2. Select **Get Started**.
The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.
5. Read the End User License Agreement (EULA) carefully and then check **Agree**.
6. Download the containerized OT Discovery dependencies package and the installer package.

Note: Download the OT Discovery Collector containerized package that is compatible with your machine's OS.

7. Decompress the downloaded packages.

Note: In case you're installing on a Debian OS, install Docker for Debian OS. For more information, see [Install Docker Engine on Debian](#) .

8. Set up the latest version of docker:

```
sudo apt install docker-ce docker-ce-cli containerd.io
docker-buildx-plugin docker-compose-plugin
```

- Run the `build-rabbit-and-mongo-images.sh`.

```
chmod +x build-rabbit-and-mongo-images.sh
./build-rabbit-and-mongo-images.sh
```

This builds the containers for RabbitMQ and MongoDB.

- Copy the RabbitMQ and MongoDB containers into the `OCI_compliant_images` directory.

```
sudo cp offline-console-mongodb_latest.tar.gz
offline-console-rabbitmq_latest.tar.gz
/home/serviceadmin/OfflineConsoleInstaller/OCI_compliant_images/
```

- Copy the RabbitMQ and MongoDB containers into the Installer folder.

- Install Podman:

```
sudo apt install podman podman-compose
```

- Install the offline console:

```
chmod +x offline-console-init.sh
./offline-console-init.sh
```

Install containerized OT Discovery components on Rocky 10

Install the containerized packages for the Discovery Console for OT and the OT Discovery Collector onto a machine with Rocky 10 OS.

Before you begin

Role required: admin

Procedure

- On your ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page.
- Select **Get Started**.
The **Download & Deploy OT Discovery** page opens.
- In the first section of the setup, select **Download & Deploy OT Discovery**.
- Select **Configure**.

The **Downloads** page opens.

- Note:** Review the End User License Agreement (EULA) and select **Agree** before proceeding. Consider moving these actions to separate steps.

- Download the containerized OT Discovery dependencies package and the installer package.

- Note:** Download the OT Discovery Collector containerized package that is compatible with your machine's OS.

- Decompress the downloaded packages.
- Run the `Build the Offline Installer` script.
This creates a ZIP archive that contains an offline installer that can be used in air-gapped networks.
- After the installer is complete, move the ZIP archive to the target system for installation.

9. Decompress the offline installation archive.

10. Copy the required files:

```
scp -r offline-console-init-support-files-main
serviceadmin@<Console IP Address>:/home/serviceadmin
```

```
scp -r OfflineConsoleInstaller serviceadmin@<Console IP
Address>:/home/serviceadmin
```

```
serviceadmin //@<password>
```

```
ssh serviceadmin@<Console IP Address>
```

11. Install Podman:

```
dnf install -y zip podman
```

12. Set up the latest version of Docker:

a. Update system:

```
sudo dnf update -y
```

b. Install the dnf plugins package, which is required for config-manager:

```
sudo dnf install -y dnf-plugins-core.
```

c. Add the official Docker repo: .

```
sudo dnf config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
```

13. Install Docker.

```
sudo dnf install -y docker-ce docker-ce-cli containerd.io
docker-buildx-plugin docker-compose-plugin
dnf install -y which
```

14. Unzip the Discovery Console for OT dependencies package and build the containers for RabbitMQ and MongoDB:

```
chmod +x build-rabbit-and-mongo-images.sh
./build-rabbit-and-mongo-images.sh
```

15. Copy the RabbitMQ and MongoDB containers into the Installer folder:

```
sudo cp offline-console-mongodb_latest.tar.gz
offline-console-rabbitmq_latest.tar.gz
/home/serviceadmin/OfflineConsoleInstaller/OCI_compliant_images/
```

16. Install the offline console:

```
chmod +x offline-console-init.sh
./offline-console-init.sh
```

Requirements for Discovery Console for OT installation

For remote deployment at a facility or on a network, verify that the following requirements are met before installing the Discovery Console for OT.

Infrastructure requirements

You must have a Linux operating system installed that can operate in a virtualization environment or on a Bare-metal server. Install the Discovery Console for OT on a virtual machine.

Note: After installing the Console and the Operating System (OS) on a virtual machine (VM), the VM must have a minimum of 10-GB of unused space available.

System requirements

The table lists the minimum resource requirements for the Discovery Console for OT. For more information, see [OT Discovery System Resources](#).

System Requirements

Component	System Requirements
Discovery Console for OT	• 16 GB RAM • 100 GB Hard drive • 2 CPUs

Note: The required dependency version has been changed to .NET 10 from .NET 8

Network requirements

The Discovery Console for OT requires the following ports to be open inbound (from the connection source to the Console) to operate.

Network requirements

Ports	Description
TCP 5671	Used by Discovery Sensor for OT to communicate with the Discovery Console for OT. This port is used by the Sensor to report data and receive configuration updates from the Console.
TCP 8443	Used to connect to the Discovery Console for OT Web interface. This port is used by the API.
TCP 5002	Enables Sensors to communicate with the Discovery Console for OT to receive updates.
TCP 443	Used for network communication from the Console to a ServiceNow instance or MID Server via the Service Graph Connector for OT Discovery.
UDP 123 (Required)	Enables Sensor devices to synchronize time (real-time clock) with the Discovery Console

Network requirements (continued)

Ports	Description
	for OT to verify that the time associated with reported data and events is both precise and accurate. Note: Without port UDP 123 open on the firewall, the clocks of Sensors drift apart from the clock of the Console. When clock drift is present, various features that rely on precise clock synchronization don't work as expected.

Note: If there are problems accessing the Discovery Console for OT, check the firewall rules and unblock the specific IP addresses and ports used for the installation. If you have any errors or difficulties while using the Discovery Console for OT, [contact Customer Service and Support](#) 

Discovery Console for OT configuration wizard

The Discovery Console for OT now provides a configuration wizard to guide you through your initial setup and configuration of the Console. If you choose to use the interactive configuration wizard after logging into the Console, it alerts you automatically to upload a Console license. For more information, see [Use the Discovery Console for OT interactive configuration wizard](#).

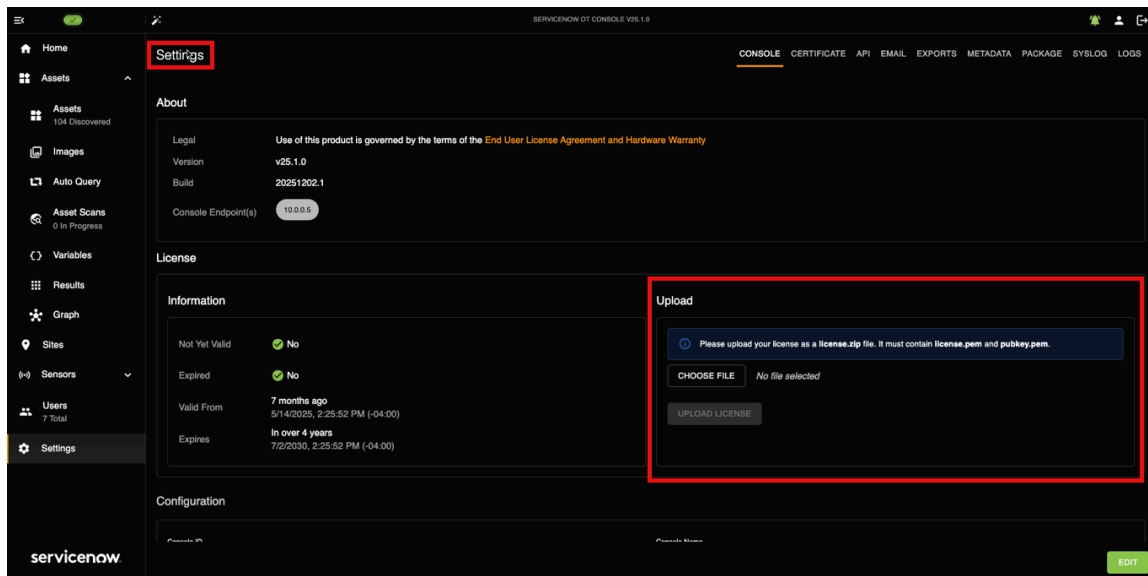
Discovery Console for OT license

Note: Before you can use the Console, you must have a license. Request a Console license from your ServiceNow account representative.

When you first sign into the Console, a warning banner alerts you that there is no license. To upload a license for the Discovery Console for OT, do the following:

1. From the Home page, navigate to the Settings page.
2. On the Settings page in the License section, select the **Upload License** button.
3. Upload your license as a .zip file.
4. Verify the ZIP file contains the license.pem and pubkey.pem files.

Once you have uploaded your license, you can use the Console.



Console features that require a license

It is important to understand that certain features are rendered inactive if the Discovery Console for OT license is expired. After the license expires, the locking mechanism is triggered and deactivates these features. No data is lost in the background. When a valid license is uploaded, the you can start or continue working. When the license is about to expire, the Console displays a warning banner as an alert.

The license:

- Enables the ability to run Auto Query and asset scans (inactive on expiration).
- Enables the consumption of network connection data (inactive on expiration).
- Enables the creation and viewing of API tokens (inactive on expiration).
- Enables the export of collections (for example, assets) to files (inactive on expiration).

Note: You can't export RAW XML results if your Console license is invalid (absent or expired).

Install a Linux operating system

Install a Linux operating system on a virtual machine and then install the Discovery Console for OT on the same VM.

Before you begin

Role required: admin

About this task

- Install the distribution with minimal configuration, including an SSH server, and confirm the VM supports AVX/AVX2 instructions.
- Allocate 16 GB of RAM for installation. For more information, see [OT Discovery System Resources](#) or [Requirements for Discovery Console for OT installation](#).

Procedure

Install any of the following Linux distributions.

Compatible Linux distributions

OS	Description
RedHat Enterprise Linux (RHEL) 8.x, 9x, and 10x	See https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10#Installing%20RHEL 
Rocky 8.x, 9x, and 10x	See https://docs.rockylinux.org/10/guides/installation/ 
Debian 12 and 13	See https://www.debian.org/releases/testing/amd64/ 
Ubuntu 22.04 and 24.04	See https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview 

Install the Discovery Console for Operational Technology (OT)

Install the Service Graph Connector for OT Discovery before accessing the Discovery for OT packages. You must also install a Linux distribution on the same machine the Discovery Console for OT is installed on.

Before you begin

Role required: admin

About this task

Once the Linux OS is installed on the device with the Discovery Console for OT installed on it, do the following.

-  **Note:** When running the installation for any of the supported distributions, you'll want to use the minimal installation, no desktop environment, but include an SSH server in the package selection.

Important when setting up your VM environment:

- Verify that the CPU settings for the VM are set to `host`; the hypervisor/host system must include support for the AVX/AVX2 instruction set.

-  **Note:** Be sure you have set this correctly; otherwise, MongoDB may crash when you attempt to restart the VM.

- Allocate 16 GB RAM for the Linux installation.
- The OT Discovery Console requires a minimum of 100 GB of storage. Increase the storage based on Deep packet capture inspection requirements. For more information, see [OT Discovery deployment scenarios](#)
- You must be on a VM to access images in the Discovery Console for OT.

Procedure

1. On your ServiceNow instance, navigate to the [Service Graph Connector for ServiceNow Operational Technology \(OT\) Discovery](#) Guided Setup page.
2. Select **Get Started**.
The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.

servicenow
All Favorites History Workspaces Admin
Download & Deploy OT Discovery

Download & Deploy OT Discovery

To begin discovery in your environment, download the OT Discovery packages and deploy them in your network. Contact your Account Team or OT Solution Consultant to get access to the license files. This [End User License Agreement](#), dated December 4, 2025 supersedes any other version.

Downloads

OT Discovery Console Standard Packages	
Discovery Console Package (zip)	Download Link

OT Discovery Console Containerized Packages	
Discovery Console Dependencies (zip)	Download Link
Discovery Console Containerized Package (zip)	Download Link

OT Discovery Collector - Windows	
Collector Installer (iso)	Download Link
Collector Installer (app, signed)	Download Link

OT Discovery Collector - Linux (Containerized)	
Collector Installer (tar.gz)	Download Link

OT Discovery Collector - Linux	
Collector Installer (tar.gz)	Download Link

OT Discovery Sensor Packages	
Discovery Sensor Package (iso.zip)	Download Link
Discovery Sensor Update Package (iso.zip)	Download Link

OT Discovery Documentation	
OT Discovery Documentation	Download

Note: For downloading and installing the containerized Console and Collector packages, see [Air-gapped networks and OT Discovery installation](#).

5. On the OT Discovery Collector page, download the Discovery packages:

- First download and install the Discovery Console for OT package.
- After the Console, download and install the Discovery Sensor for OT package.
- Finally, download and install the OT Discovery Collector package that is compatible with your machine's OS.

Note: Read the End User License Agreement (EULA) carefully and then check Agree.

6. From the Discovery Console for OT install package, unzip the ConsoleInstaller ZIP file.

7. Use the secure copy protocol (SCP) to move the ConsoleInstaller folder onto your Linux server.

a. Push to the console:

```
scp -r ConsoleInstaller serviceadmin@IP:/home/serviceadmin$
```

For example:

```
$ scp -r ~/Users/Zelda/Downloads/ConsoleInstaller SL
serviceadmin@192.168.2.2:/home/serviceadmin
```

Note: The ConsoleInstaller folder name can vary if so desired.

b. Pull from the user computer:

```
$ scp -r $USER@$IP:~/ConsoleInstaller /home/serviceadmin/
```

8. Run the console initiation script (console.init) via SSH.

a. Enter the password when prompted.

```
ssh serviceadmin@$IP
```


Generate a certificate

Generate a certificate to use with the Discovery Console for OT or upload your own certificates. This certificate allows the Console to boot up.

Before you begin

- Note:** If you choose to do so, you can create your own certificate if it is required by your company's policies.

Role required: admin

About this task

After the Discovery Console for OT is installed, there are default, preloaded certificates that power up the Console. However, following this initial boot, it's recommended that you use the Console to generate a new Certificate Authority (CA). This task describes your options for generating the Console CA.

- Note:** You can also select the link **Download Console Certificate Bundle (.zip)**. For more information, see the table.

Procedure

1. Navigate to the Discovery Console for OT **Settings > Certificate** tab.
2. Generate a new bundle, upload an existing bundle.

- Note:** You're not obligated to use the ServiceNow provided certificates and you may choose to use your own.

Option	Description
Generate a new bundle	- Under Update Certificate, select Generate New Bundle. - Select the Generate Bundle button.
Upload an existing bundle	- Under Update Certificate, select Upload Bundle (.p12). - Use the Choose File button and select the bundle to upload. - Enter a Bundle Password. - Select the Upload Bundle button.
Download Console Certificate Bundle (.zip)	The bundle contains the Console's Certificate and the web browser certificate. These certificates establish trust between these applications and confirm their communications are secure and encrypted.

- Note:** Generating or uploading a certificate also updates any current certificates.

Result

A certificate is generated. The Discovery Console for OT reboots.

Upgrade the Discovery Console for OT

These are the instructions for upgrading the Discovery Console for OT. The scope of this document does not include how to upgrade the containerized version of the Console.

Before you begin

You must have the latest version of the Console already been installed on one of the supported Linux distributions.

- Note:** After the March 2026 GA release of the Console, the version of the .Net runtime has been changed from 8.x to 10.x since the 8.x version has an End of Support date of November 10, 2026.

The Console packages now require .Net 10.x. The console-upgrade.sh script included with consoleinstaller builds of 20260527.3 or later attempts to install this dependency before making any other changes to the system. This requires internet connectivity for the upgrade installation. If the script determines .Net 10 is not present on the system and is unable to install it, it exits before attempting to upgrade to the new set of Console packages.

Also, Rabbit 4.3 was released after the GA release. This script does not attempt to make any changes to accommodate a newer Rabbit version, because:

- the system is still running the version installed at the time of the original Console installation, **OR**,
- if Rabbit was upgraded after that, this was intentionally done by the end user, and this end user has already updated the Rabbit version.

Role required: admin

Procedure

1. Transfer the new `consoleinstaller` package over to the system hosting the Console.
2. Unzip the package by typing `unzip [name of console installer package]`.

Note: If you run this command in a directory where there is already a `ConsoleInstaller` folder present, you're prompted with: `replace ConsoleInstaller/docs/codeowners.md? [y]es, [n]o, [A]ll, [N]o, [r]ename: Type A` followed by Enter/Return to continue unzipping the files.

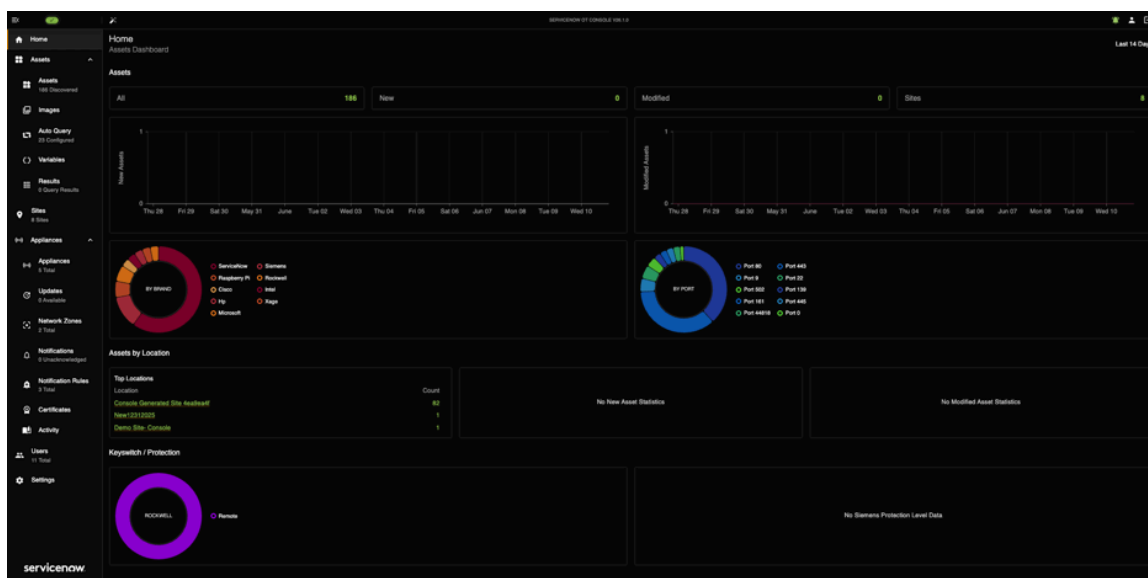
3. Change directory to the `ConsoleInstaller` folder by typing `cd ConsoleInstaller`.
4. Type `chmod +x console-upgrade.sh` to make sure the upgrade script is set to be executable.
5. The Console upgrade script needs to run with root privileges.

Include desired level of detail for using either `su` or `sudo` to do that.

6. Run the upgrade script by typing the following command: `/bin/bash console-upgrade.sh`.
Depending on the current state of the system, you may be prompted with a few questions to complete the upgrade process. The console upgrade script can run the latest migration scripts automatically with no user input needed. This requires Console installer program version 20260601.8 or later for `devslim`.

Use the Discovery Console for OT pages

Get started with the Discovery Console for OT application after it is installed and configured.



Navigating the Console pages

The Discovery Console for OT is organized into multiple pages navigated by the side navigation panel. Each page displays specific tasks you can accomplish. Every page contains information and step-by-step procedures for using the Discovery Console for OT to query and inventory in your OT environment.

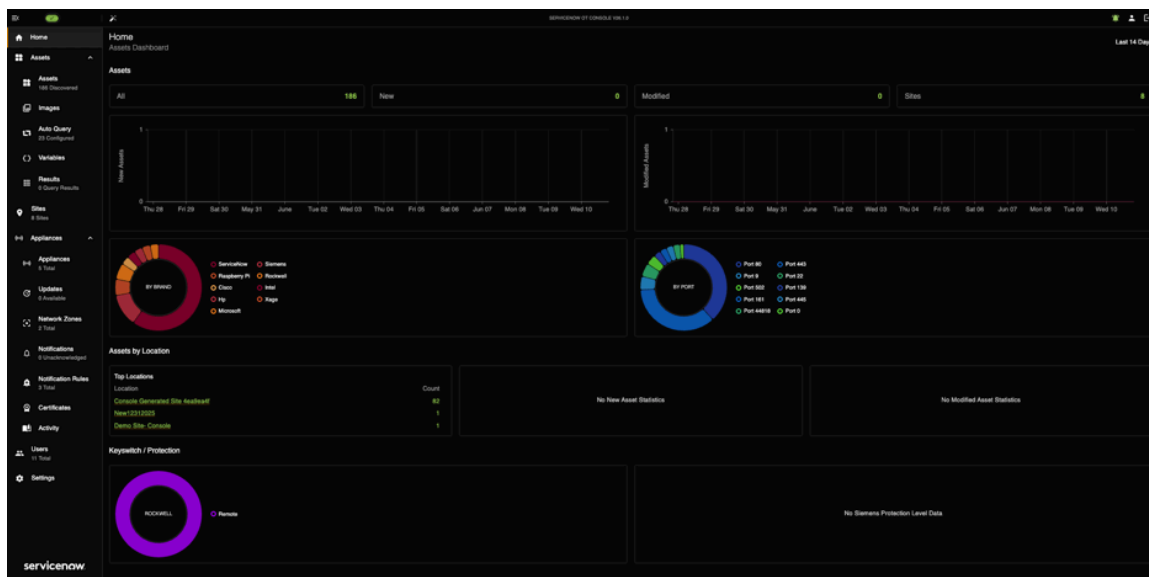
The next sections describe the Discovery Console for OT pages and how to use the Console's features.

Home page

The Home page on the Discovery Console for OT provides a dashboard overview of the assets and sites on your current system.

In the navigation menu, you can select the Assets and Sensors pages to reveal sub-menus. You can select Sites, Users, and the Settings items for more data.

The Console opens to the Home page.



The **Home** page is made up of a left-hand, expandable navigation menu and a main area; that is, the Assets Dashboard. The dashboard is divided into the following sections.

- Assets section
- Assets by Location section
- KPI cards section

Assets

The Assets section gives you an overview of the assets and sites available in your system, organized by widgets. The widgets are the following:

- **All:** List of all the assets in your system.
- **New:** List of the most recently discovered assets.
- **Modified:** List of the most recently edited or updated assets.
- **Sites:** List of all current sites.

By selecting the **All** widget, you can view the list of all the assets in your system. The **New** widget takes you to a list of the most recently discovered assets. The **Modified** widget takes you to a list of the most recently edited or updated assets. The **Sites** widget lists all current sites available in the Console.

Underneath these widgets are two graphs: **New Assets** and **Modified Assets**. The graphs display asset information organized by date.

Under these graphs are the **By Brand** and **By Port** graphs. The **By Brand** graph breaks up your assets according to brand. The **By Port** graph breaks up your assets based on the available ports that they're connected to. Selecting a section on either of these images takes you to the asset list filtered by the selected brand or port.

The following image shows an example of the data that you can find in the Assets section.



Assets by Location

The Assets by Location section provides the number of assets according to the available site. The location of an asset is dependent on the Site's IP ranges that you define when creating a site. For more information about creating a site, see [Add a Site](#).

The **Top Locations** widget ranks each location based on its number of assets. The **New Assets** widget calls out any recently discovered assets by Site. The **Modified Assets** widget calls out recently edited or updated assets by site.

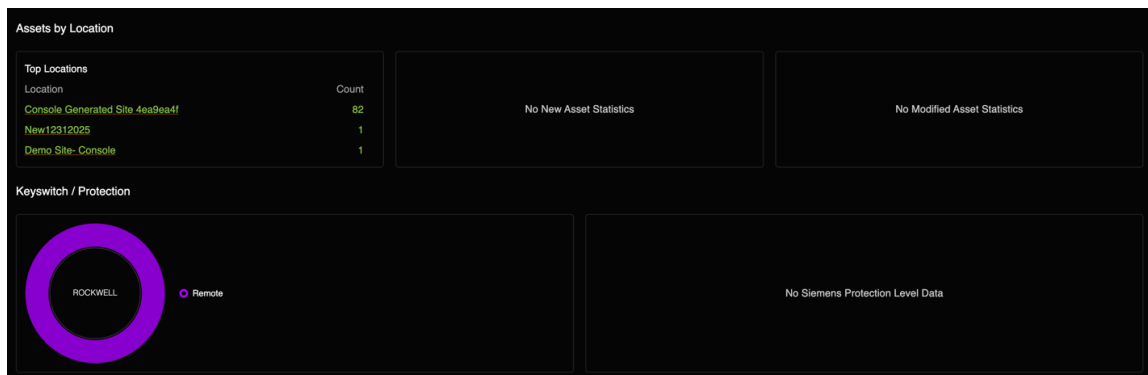
The following image shows an example of the data that you can find on the Assets by Locations section.

Assets by Location			
Top Locations		New Assets	
Location	Count	Site	Count
Charlottesville	131	Ashburn	2
Ashburn	2		
Houston	1		
Modified Assets			
Site	Count		
Charlottesville	4		
Ashburn	2		

Keyswitch / Protection

The Keyswitch / Protection section displays any key switch security or protection that you can have for your system assets. The following image shows an example of the data that you can find in the KeySwitch / Protection section.

Note: The Keyswitch / Protection section is only available if you have data available in your system.



Assets page

The Assets page shows a list of all available assets for the Discovery Console for OT.

Note: To edit any of the fields in the Asset record, select the asset from the list and then select the Edit button. After editing, select Save to save any changes.

Assets page overview

The Assets page shows all assets that were automatically discovered along with all assets that were manually added to the system. To view the assets list, use the navigational menu on the left side of the screen and select **Assets > Assets**.

The screenshot shows the ServiceNow OT Console interface. The left sidebar contains a navigation menu with options like Home, Assets, Images, Auto Query, Variables, Results, Graph, Sites, Sensors, Users, and Settings. The main area displays a table of 104 total assets. The table has columns for Changes, Category, IP Address, Hostname, Brand, Product, Location, Ignore From Auto Query, Network Zone, Open Ports, and Images. The first few rows show assets with IP addresses like 192.168.43.80 and 192.168.40.95, all categorized as 'Unknown'.

Changes	Category	IP Address	Hostname	Brand	Product	Location	Ignore From Auto Query	Network Zone	Open Ports	Images
Asset	Unknown	192.168.43.80		Unknown			No	Default	N/A	
Asset	Unknown	192.168.40.95		Unknown			No	Default	N/A	
Asset	ICS Host	192.168.1.145		Unknown			No	Default	N/A	
Asset	Unknown	10.1.3.5		Unknown			No	Default	N/A	
Asset	Unknown	192.168.40.74		Unknown			No	Default	N/A	
Asset	ICS Host	192.168.1.146		Unknown			No	Default	N/A	
Asset	Unknown	192.168.40.11		Unknown			No	Default	N/A	
Asset	Unknown	192.168.41.157		Unknown			No	Default	N/A	
Asset	ICS Host	192.168.1.147		Unknown			No	Default	N/A	
Asset	Unknown	10.1.3.7		Unknown			No	Default	N/A	

You can add assets with the following methods.

- Sensors and Collectors perform Native discovery and populate the assets.
- Import via a CSV with assets information.
- By selecting the add icon .

Filter panel

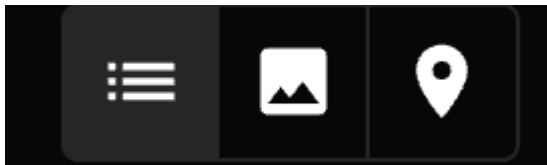
When you open the Assets page, there is a Filter panel you can use to filter which Assets appear in the list. There are preset filters which appear as tabs at the bottom of the panel. The preset filters are (you can also check the Default Tab box):

- Sites
- Presets
- Filters

Select the X at the top of the panel to close the filter. To open the panel, select the filter icon .

Views

In the top right area of the Assets list, there are different icons that control how the Assets are viewed.



The views are:

- List view
- Gallery view
- Map view

Actions

The **Actions** button provides a drop-down menu for manipulating the Assets. The formats for each are indicated next to the selection where applicable. The selectable actions are:

- Import Assets
- Import Ignore Assets (CSV)
- Export Ignore Assets (CSV)
- Export Assets (JSON)
- Export Assets (CSV)
- Update Manufacturer Data
- Update Vulnerability Data
- Update Product Mappings
- Update Purdue Levels
- Ignore Assets
- Delete Assets

 **Note:** If an action is inactive, it appears grayed out in the menu.

Next to the **Actions** button is the add icon .

Asset records

With an Asset record, you can view and edit the details of the selected asset. To view an asset record from the Assets page, select the IP address displayed for the asset. The following sections describe each section of an Asset record.

Note: When you select the add icon , this same view opens with these same sections. However, when you open an existing asset record, you have three tabs on the upper right side of the screen. The tabs are **Details**, **Images**, and **Modules**.

Identification

The Identification section contains the following fields.

Field	Description
IP Address [Required]	IP Address assigned to the asset.
Hostname	Name of the connected device. Note: The name is populated when it is configured on the device or if the DNS server is configured.
Product	Manufacturer and model of the asset.
Firmware Version	Version of the firmware installed.
Network Zone	Network zone of the asset.
MAC Address	MAC address that is associated with a given asset.
Serial Number	Serial number associated to the asset.
Ignore from Auto Query	Option to mark devices that must be ignored from the auto queries. This field is automatically set to inactive,

Classification

The Classification section contains the following fields.

Field	Description
Auto Categorization	Feature that enables the Discovery Console for OT to manage and update the Description , Category , and Operating System fields through the automatic classification system. Set to Yes or No. Note: If Auto Categorization has been enabled, then editing is turned off for the Category , Brand , Operating System , and Details fields. Users can select Edit and then modify the values during editing. To delete an asset, set Auto Categorization to No . The Delete button then appears in the right-most column allowing you to delete the asset.

Field	Description
Category	Category or classification indicates the function of the device or class that the asset belongs to. For example, Desktop, HMI, PLC, or SCADA.
Brand	Name of the manufacturer that produced the asset.
Purdue Level	N/A by default. See image of drop-down choices.
Operating System	Operating system of the asset. For example, IOS, Linux, or Windows.
Details	Section for additional details to describe the classification for this asset.

Timeline

The Timeline section contains the following dates and times related to the asset.

Timeline

Field	Description
Created	When the asset was created.
Modified	The last time the asset was modified.
Last Seen	The last time the asset was detected.
Updated	The last time the asset was updated.

Open Ports

The Open Ports section lists all open ports available on the asset that were identified by Discovery and shown on the Discovery Console for OT.

Open Ports (3)

Filter ports or services... # SERVICE

SSH (Port 22) WWW-HTTP (Port 80) HTTPS (Port 443)

Metadata

Alias _____

Description _____

Labels
Console Generated Site 4ea9ea4f

Location
Console Generated Site 4ea9ea4f

Network Interfaces

The Network Interfaces section displays the Asset's Vendor, Vendor Address, IPV4 Address, IPV6 Address, MAC Address, Gateway, and CIDR.

Network Interfaces								10 Network Interfaces
Name	Vendor Name	Vendor Address	IPV4 Address	IPV6 Address	MAC Address	Gateway	CIDR	
Red Hat VirtIO Ethernet Adapter F64BA22F-A5CB-4A4B-BAEB-D8A1AD6A027D	Proxmox Server Solutions GmbH	Braeuhaugasse 37 Vienna Vienna 1050, AT	192.168.41.123	fe80::84f5:c855:1288:3ee0	BC:24:11:01:97:56	192.168.40.1	/64	
WAN Miniport (Network Monitor) 586D65B6-5AA1-48F7-B97C-06CD088E77C84	N/A		N/A	N/A	0A:F1:20:52:41:53	N/A	N/A	
WAN Miniport (IPv6) 049E44B1-82BF-4F6B-8D06-08C0BCB1BEFD	N/A		N/A	N/A	08:73:20:52:41:53	N/A	N/A	
WAN Miniport (IP) 8FE6CD42-3115-4408-8195-68ADF9DF35D9	N/A		N/A	N/A	04:32:20:52:41:53	N/A	N/A	
Microsoft Kernel Debug Network Adapter BBE0896E-10EA-4B7A-B6AC-18B4677349FE	N/A		N/A	N/A	N/A	N/A	N/A	

Metadata

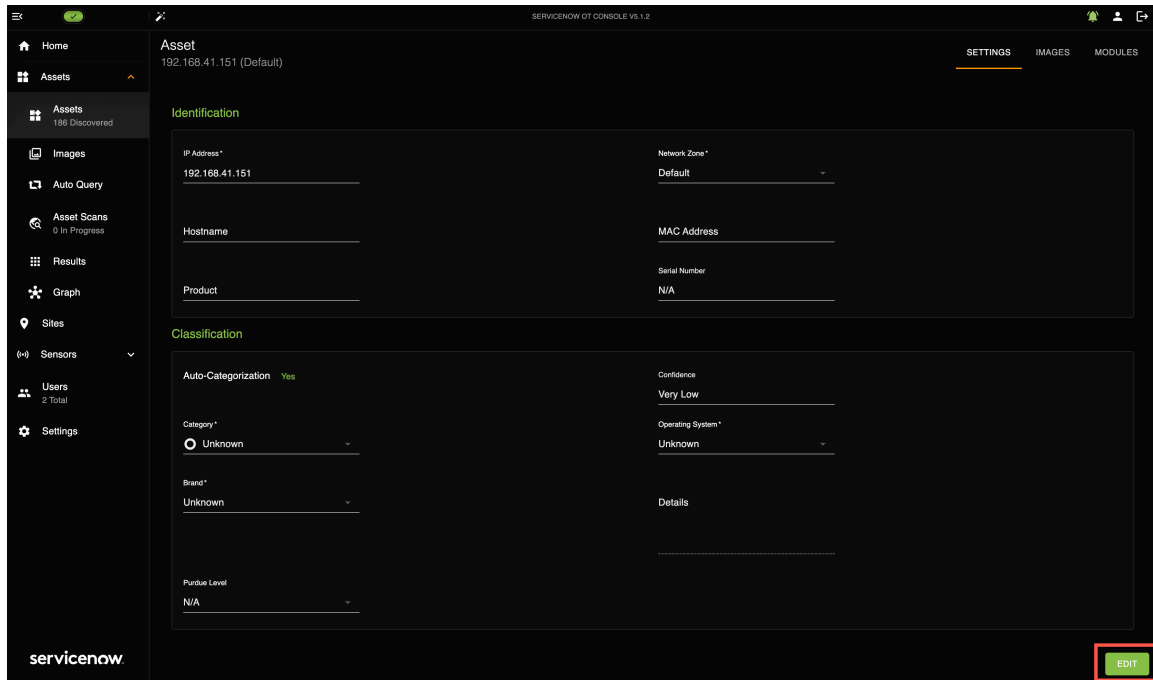
The Metadata section contains the following fields.

Field	Description
Alias	Alternate name given to the asset. Where possible, the alias is displayed instead of the IP Address or MAC address to provide a user-friendly way to identify the asset.
Description	Description of the asset.
Labels	Tag that you can add to an asset to assist in identifying and finding assets with the tagged properties within the system.
Location	Description of the physical location of the asset.

Installed software

The Installed Software section includes a list of all software installed on the asset. To add software, complete the following actions.

1. Select the **Edit** button.



2. Scroll to the Installed Software section and select **Add Software**.



3. In the Add Software modal window, enter the **Vendor**, **Product**, and **Version** (optional) of the software being added.

4. Select **Save**.

The added software displays in the Installed Software list.

Attributes

The Attributes section contains the attributes discovered by the Discovery process. To add an attribute, complete the following actions.

1. Select the **Edit** button.

2. Scroll to the Attributes section and select **Add Attribute**.



3. In the Attribute modal window, enter the **Name** and **Value** of the attribute.

4. Select **Add Attribute**.

5. Select **Save**.

MAC Addresses

The detected MAC Addresses section includes a list of all the MAC addresses that are associated with a given asset. The Real Address toggle is used to indicate that a MAC address belongs to an asset and should be considered the primary or main MAC address. Each detected MAC address in the list includes the **Vendor Name**, **Vendor Address**, **First Detected On**, and **Last Detected On** fields.

MAC Addresses					ADD MAC ADDRESS	
Real Address	MAC Address	Vendor Name	Vendor Address		First Detected On	Last Detected On
Yes	ac:84:17:42:3d:f1	Siemens AG	Werner-von-Siemens-Strasse 58 Amberg 92224, DE			

To add a MAC address, complete the following actions.

1. Select the **Edit** button.
2. Scroll down to the MAC Addresses section and select **Add MAC Address**.
3. In the Add MAC Address modal window, add the name of the MAC Address.
4. Select **Add Mac Address**.
5. Select **Save**.

Comments

The Comments section provides an area to enter additional information about the assets. To add a Comment, complete the following actions.

1. Select the **Edit** button.
2. Scroll to the Comments section and select **Add Comment**.

Comments	ADD COMMENT
----------	-------------

3. In the Add Comment modal window, enter a comment.
4. Select **Save**.

The added comment is listed in the Comments section of the asset.

Create an asset

Manually create an asset to the Discovery Console for OT.

Before you begin

Role required: admin

Procedure

1. Navigate to the **Assets** page.
2. Select the add  icon.
3. In the **Create Asset** page, fill in the following sections.
 - **Identification:** If applicable, add the following information:
 - **IP Address:** Required.
 - Hostname
 - Product
 - Firmware Version
 - Network Zone
 - MAC Address
 - Serial Number
 - **Ignore from Auto Query:** Slide toggle to set to Ignore.
 - **Classification:** If applicable, add the following information:

- **Category:** Required. Provides a pop-up list to choose from.
- **Brand:** Required. Provides a pop-up list to choose from.
- **Purdue Level:** Optional. Provides a pop-up list to choose from.
- **Operating System:** Required. Provides a pop-up list to choose from.
- **Details:** Optional.
- **Network Interfaces:** Displays available network interfaces.
- **Metadata:** If applicable, add the following information:
 - Alias
 - Description
 - Labels
 - Location
- **Installed Software:** If applicable, select the Add Software button and select the software you want to include.
- **Attributes:** If applicable, select the Add Attribute button and select the Attributes you want to include.
- **MAC Address**
- **Comments:** If applicable, add comments.

4. Select **Create Asset** to create an asset or select **Cancel** to discard your entries.

Result

The asset is created and added to the Assets page.

Deleting assets in bulk

Filter assets and do a bulk deletion in the Discovery Console for OT.

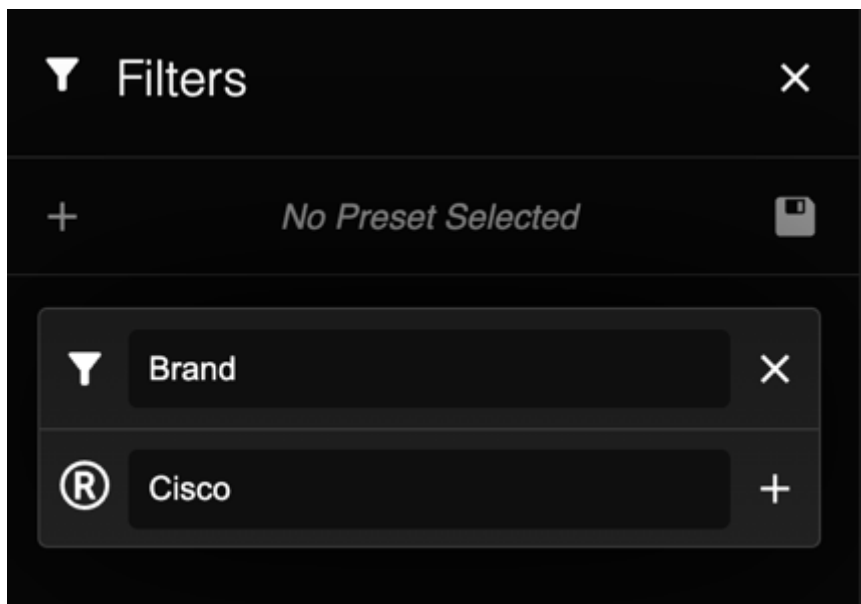
Before you begin

Role required: admin

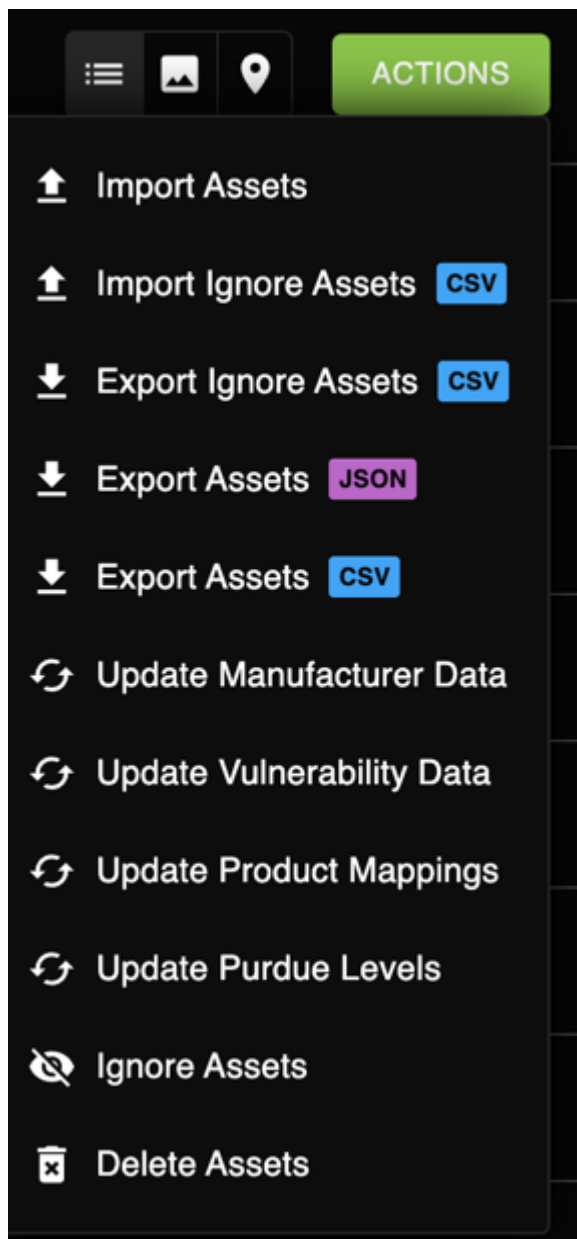
Procedure

1. Navigate to the Assets page.
2. In the Filters pane, select the bottom tab, **Filters**.
3. Select the plus sign at the top of the pane.
4. In the new entry field, select a filter type from the pop-up menu by selecting the down arrow icon .

For example, if you select Brand, a second entry field options and provides a pop-up list of brands. You can select more than one type of filter and the associated list, but you can only delete one group of assets.



5. After you have filtered your assets, select **Enter**.
The selected assets are set in the filter pane.
6. Select the **Action** button.



7. Select **Delete Assets**.

You're prompted to confirm deleting assets.

Result

The bulk deleted assets are no longer in the Assets table.

Import or export assets

You can import or export assets, and ignored assets, to either CSV or JSON formats.

Before you begin

Role required: admin

Procedure

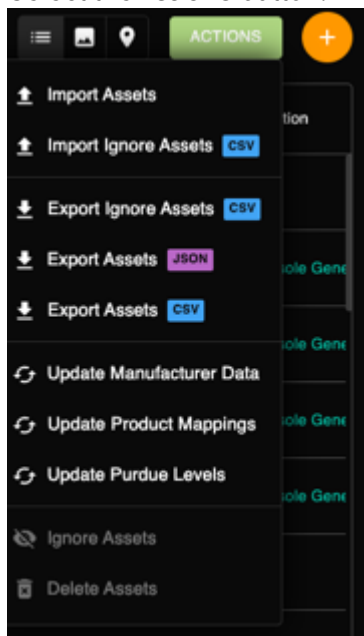
1. Navigate to **Assets > Assets** page.

The list of current assets displays on the page.

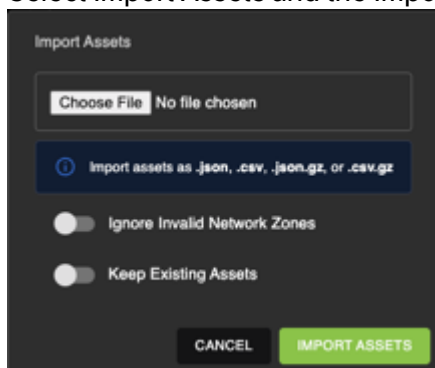
2. You can import/export all listed assets or you can filter the list using the Filter panel, selecting the Filter tab.
For more information, see [Assets page](#).

Import assets

3. Select the **Actions** button.



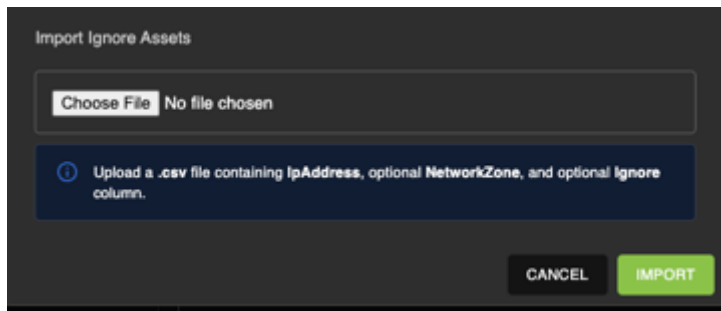
4. Select Import Assets and the Import Assets window opens.



The window lists the format you can import to the Console. You can also toggle the available settings in the window to activate them:

- Ignore Invalid Network Zones
- Keep Existing Assets

5. When you select Import Ignore Assets, the prompt window opens and displays the additional required information needed.



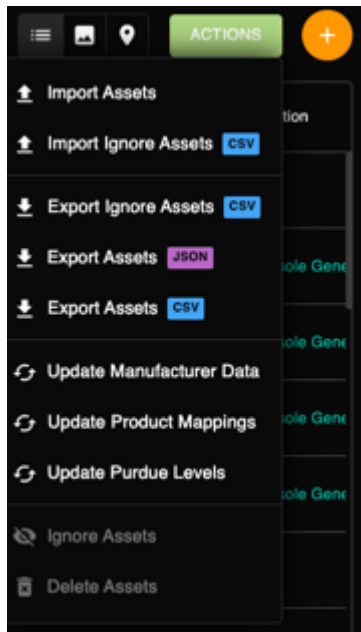
Note: The assets file must be in CSV format to upload to the Console.

6. Other actions and formats you can select from the **Actions** menu are:

- Export Ignore Assets (CSV)
- Export Assets (JSON)
- Export Assets (CSV)

Export assets

7. Select the **Actions** button.



8. Select Export Assets by the format you want the output to be.

Choose to export either .csv or json asset files. If you don't choose a specific asset or assets, all asset information is exported.

9. Use the Filters panel to sort the assets you want to export.

In this image, the assets are filtered by the general type Purdue level and the more specific Level 2.

Last Changes	Category	IP Address	Hostname	Brand	Product
New Asset	ICS Host	192.168.1.142		Unknown	
New Asset	ICS Host	192.168.1.145		Unknown	
New Asset	ICS Host	192.168.1.149		Unknown	
New Asset	ICS Host	192.168.1.148		Unknown	
New Asset	ICS Host	192.168.1.147		Unknown	
New Asset	ICS Host	192.168.1.146		Unknown	
New Asset	ICS Host	192.168.1.143		Unknown	
New Asset	ICS Host	192.168.1.144		Unknown	

- From the Actions menu, select Export Assets for the desired format, either .json or .csv. The filtered assets are exported.

Images page

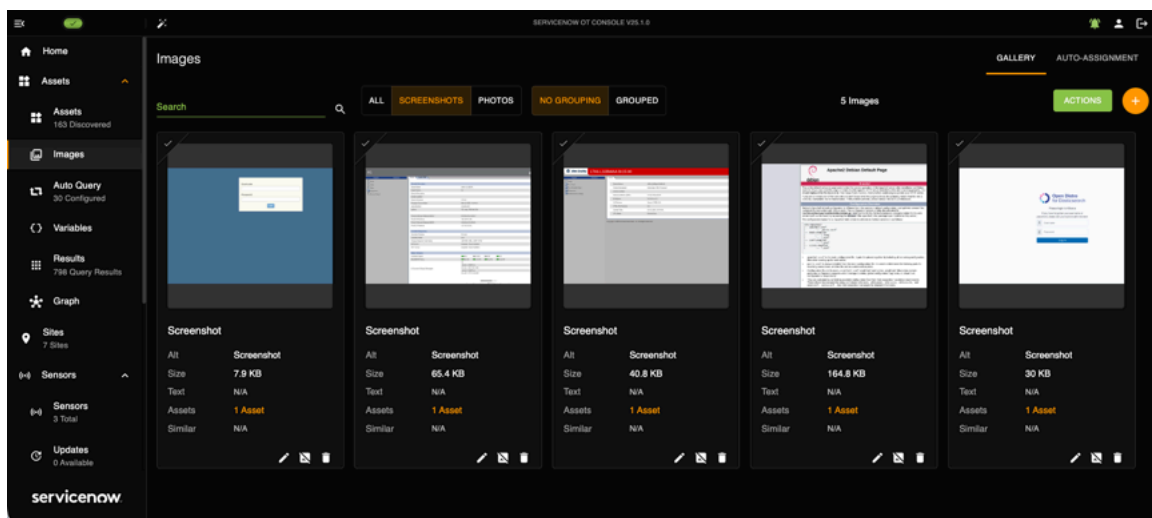
The Images page contains the images related to your Discovery Console for OT assets.

On the Images page, you can view, add, and manage photos and screenshots captured during the Discovery process related to your assets on the Console.

Note: When you import any assets, image data aren't imported.

The Images page allows you to search for an image. The page has the following tabs:

- Gallery** tab: Displays images.
- Auto-Assignment** tab:

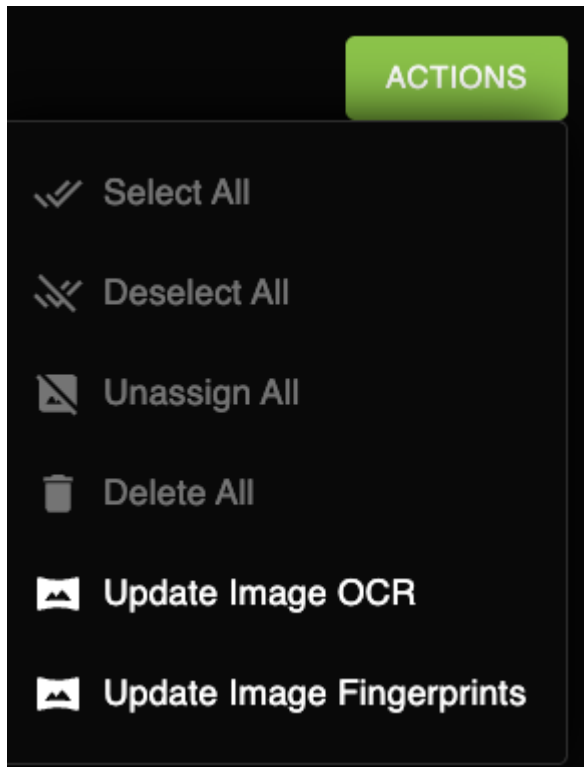


Gallery tab

The Gallery tab shows different views of the images:

- All: View all images.
- Screenshots: View only screenshot images
- Photos: View only photo images
- No Grouping
- Grouping

On the Gallery tab, select the **Actions** button and select from the drop-down menu.



Select the add icon  to browse and upload images. You can also just drag and drop the image on the window.

Auto-assignment tab

Under the **Auto-Assignment** tab, you can select the add icon  and open the **Edit Auto-Assignment Profile**.

To add an image, select the add icon .

To delete an image, select the delete icon .

i Note: To capture screenshots during the Operational Technology Discovery process, the Full Web Extractor Auto Query needs to be selected and executed. This captures the screenshots over ports 443 and 80 and extracts the content from the web pages.

Auto Query page

The Auto Query page contains the automatic asset queries for the Discovery Console for OT.

Auto Query

The Auto Query page contains a list of all the automatic asset queries available for your system. Each Auto Query is displayed in columns with the following headings and information.

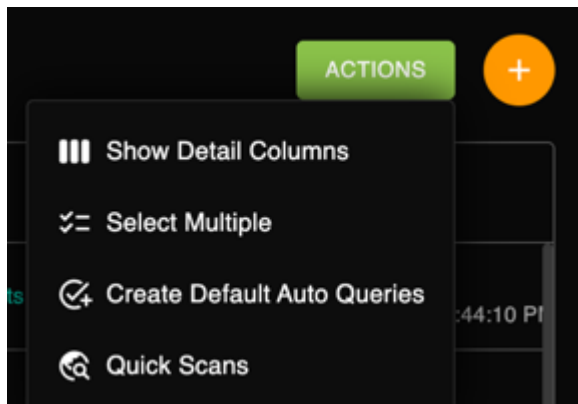
- Name
- Enabled
- Status
- Sensors
- Recurring
- Targets
- Queried
- Ignored
- Skipped
- Run Query
- Created On
- Updated On
- Last Executed On
- Completed
- Delete

The following image shows an example of the Auto Query page.

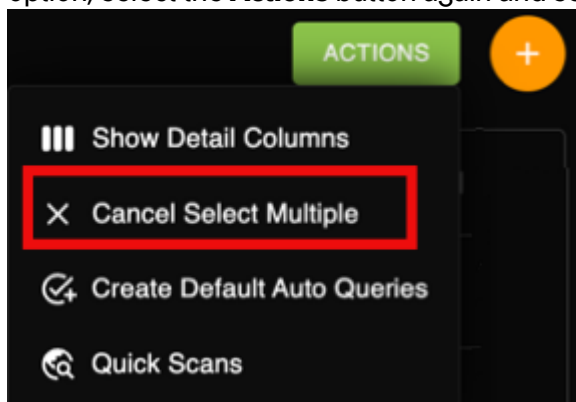
Name	Enabled	Status	Sensors	Recurring	Targets	Queried	Ignored	Skipped	Run Query	Created On	Updated On
AutoQuery_20251231_...		Idle	N/A	Just Once	0 Assets	N/A	N/A	0 Assets		23 days ago 12/31/2025, 7:10:09 AM (-05:00)	23 days ago 12/31/2025, 7:10:09 AM (-05:00)
AutoQuery_20251231_...		Idle	N/A	Just Once	0 IPs	N/A	N/A	0 IPs		23 days ago 12/31/2025, 7:01:12 AM (-05:00)	23 days ago 12/31/2025, 7:01:12 AM (-05:00)
AutoQuery_20251231_...		Idle		Just Once	0 IPs	0 IPs	N/A	0 IPs		23 days ago 12/31/2025, 6:59:34 AM (-05:00)	23 days ago 12/31/2025, 6:59:34 AM (-05:00)
AutoQuery_20251230_...		Idle	N/A	Just Once	0 Assets	N/A	N/A	0 Assets		24 days ago 12/30/2025, 1:52:03 PM (-05:00)	24 days ago 12/30/2025, 1:52:03 PM (-05:00)
Full_Web_Extractor_2...		Idle	N/A	Every 3 Days	0 Assets	0 Assets	N/A	104 Assets		25 days ago 12/29/2025, 9:12:19 AM (-05:00)	25 days ago 12/29/2025, 9:12:19 AM (-05:00)
SNMP_20251229_141...		Idle	N/A	Every 7 Days	0 IPs	N/A	N/A	0 IPs		25 days ago 12/29/2025, 9:12:19 AM (-05:00)	25 days ago 12/29/2025, 9:12:19 AM (-05:00)
Console_Hostname_L...		Idle	N/A	Every 1 Day	0 Assets	N/A	N/A	0 Assets		25 days ago 12/29/2025, 9:12:19 AM (-05:00)	25 days ago 12/29/2025, 9:12:19 AM (-05:00)
Location_Set_2025122...		Idle	N/A	Every 1 Day	0 Assets	N/A	N/A	0 Assets		25 days ago 12/29/2025, 9:12:19 AM (-05:00)	25 days ago 12/29/2025, 9:12:19 AM (-05:00)
Discovery_20251229_...		Idle	N/A	Every 7 Days	0 IPs	N/A	N/A	0 IPs		25 days ago 12/29/2025, 9:12:19 AM (-05:00)	25 days ago 12/29/2025, 9:12:19 AM (-05:00)
PB_banner		Idle	N/A	Just Once	0 Assets	0 Assets	N/A	104 Assets		12/11/2025, 12:44:10 PM (-05:00)	12/11/2025, 12:44:10 PM (-05:00)

Note: When a query is enabled but not running, the Status column displays idle icon to indicate it is idle. When related or all Sensors are offline, the All Sensors Offline icon displays.

Use the drop-down **Actions** button to select additional options.



- **Show Detail Columns:** Toggles between Show and Hide. When showing the Detail Columns, additional columns display on the page. The additional columns shown include:
 - Run Count
 - Last Run Started
 - Last Run Ended
 - Next Scheduled Run
 - Current Sites
 - Last Delay
 - Exec Time
- **Select Multiple:** Opens check boxes by each query in the list. You can check a box and the **Delete Selected** option is activated. This option deletes the selected queries. To turn off this option, select the **ACTIONS** button again and select **Cancel Select Multiple**.



- **Create Default Auto Queries:** There are 5 default queries to choose from. Selecting this option opens the Create Auto Queries window. Select from the following default auto queries:
 - **Console Hostname Lookup:** Reverses the DNS look up performed by Console.
 - **Asset ICS Discovery:** Finds the ICS assets based on common open ports and queries using native protocols.
 - **Location Set:** Sets a label and a location field using the Site name.
 - **SNMP:** Queries to discover SNMP service. This tries only the SNMP port.
 - **OS Detection:** Use with caution, especially in production environments. This query can disrupt or crash poorly configured or sensitive assets. Queries Linux / Windows endpoint for any discoverable services.

- **Quick Scans:** When selected, this selection displays a list of any current Quick Scans. You can create a Quick Scan by selecting the add icon . Set the parameters of the Quick Scan in the Create Quick Scan page. Quick Scans are meant to run quickly and only once. Quick Scan targets can be assets selected by their URLs, IP Addresses, or IP ranges. For more information on Quick Scans, see [Create a Quick Scan](#).

Create an Auto Query

Create an Auto Query that you can run on demand for different Discovery Console for OT Assets.

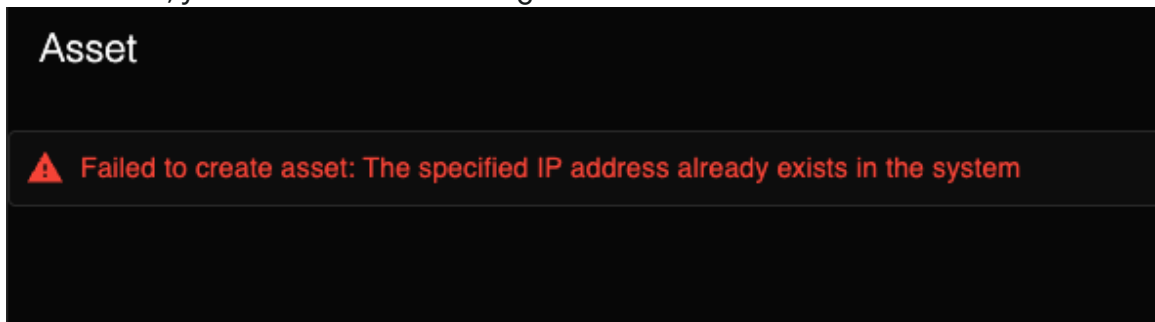
Before you begin

Role required: admin

Procedure

1. Navigate to **Assets > Auto Query**.
2. Select the add icon .
3. For the Identification section, use the automatically provided name or create your own name.

- Note:** If you use an IP address that is already in the system as the new Asset identification, you receive an error message.

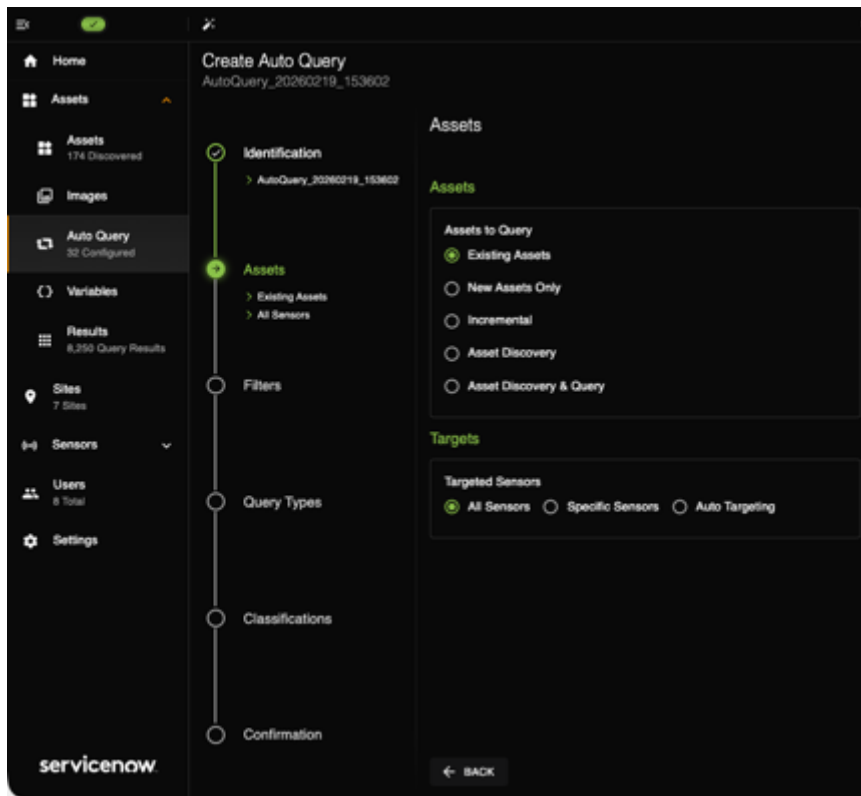


Be sure to use an IP address that is not in the system already.

4. Select **Next**.
5. In the Assets section, choose from Assets and Targets.
The available **Assets** are:
 - Existing Assets
 - New Assets Only
 - Incremental
 - Asset Discovery
 - Asset Discovery & Query

The default Asset selection is **Existing Assets**.

When **Existing Assets** is selected for a query, the query uses the asset's IP address and Network Zone as its unique identifier. This allows the asset's IP address to exist across multiple Network Zones.



6. Targets refers to Sensors and Collector.

The available **Targets** are:

- All Sensors
- Specific Sensors
- Auto Targeting

The default Targets selection is **All Sensors**. **All Sensors** uses all available Sensors and Collectors for the query. **Specific Sensors** uses only the selected Sensor and Collectors for the query. **Auto Targeting** tries to intelligently assign targets to Sensors and Collectors based on the query. It helps manage complex deployments.

7. Select **Next**

8. In the Filters section, select the filters as needed.

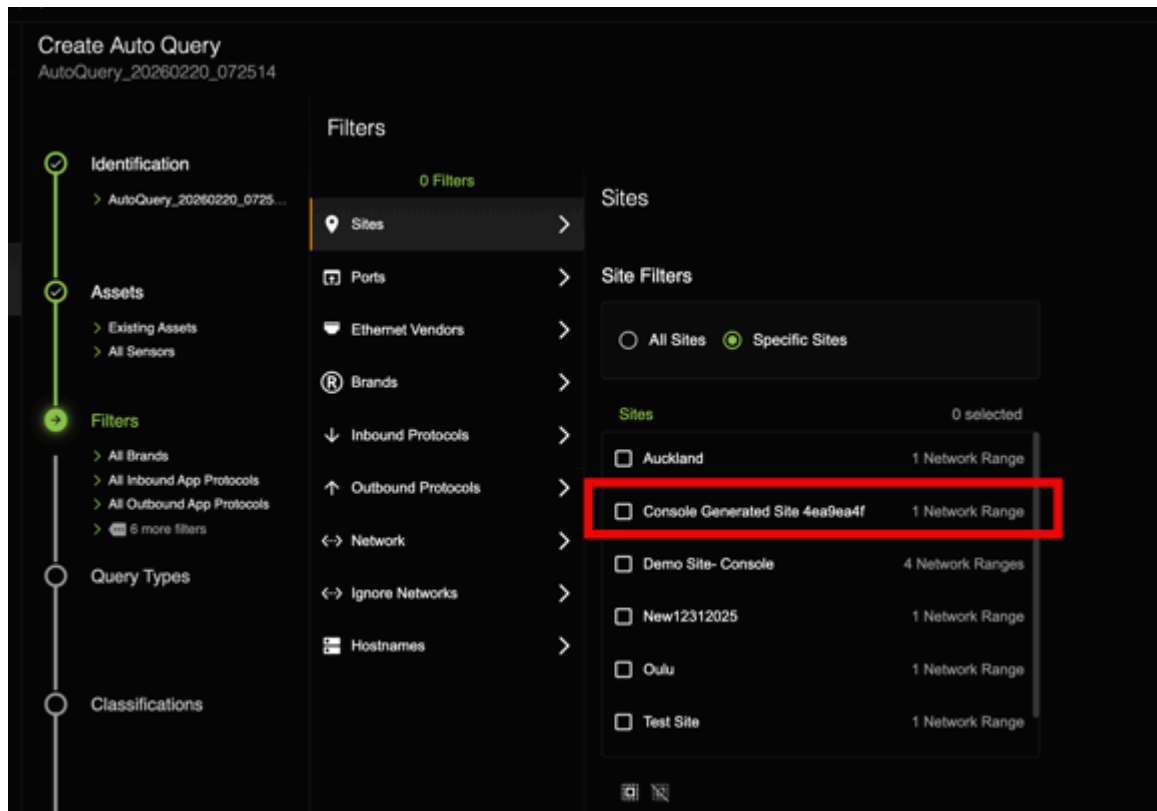
These filters help with the query selections. Filters include the following categories.

Note: Some options in this section are only visible when the Assets selection is set to Existing Assets or Incremental. When the selection is Asset Discovery or Asset Discovery & Query, a few options are inactive.

○ **Sites**

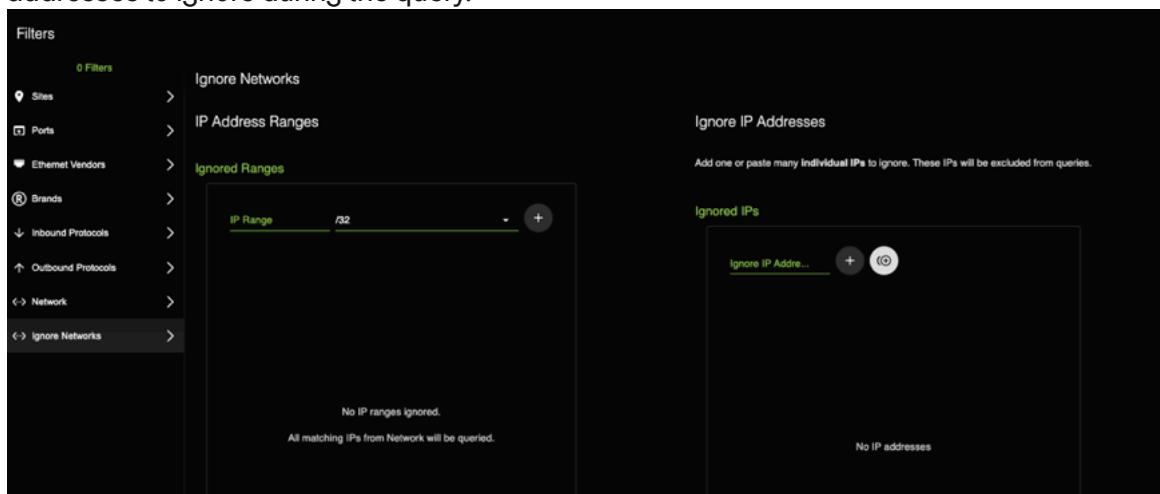
Site rules override global behavior when the Site filter is selected. If no site rules matches the Asset, the query skips the Asset.

Note: The Console automatically generates a default site. This is in case no Sites have been previously created. You can select the Console-generated site when using the Sites filter to select specific sites.



- Ports
- Ethernet Vendors
- Brands
- Inbound Protocols
- Outbound Protocols
- Network
- Ignore Networks

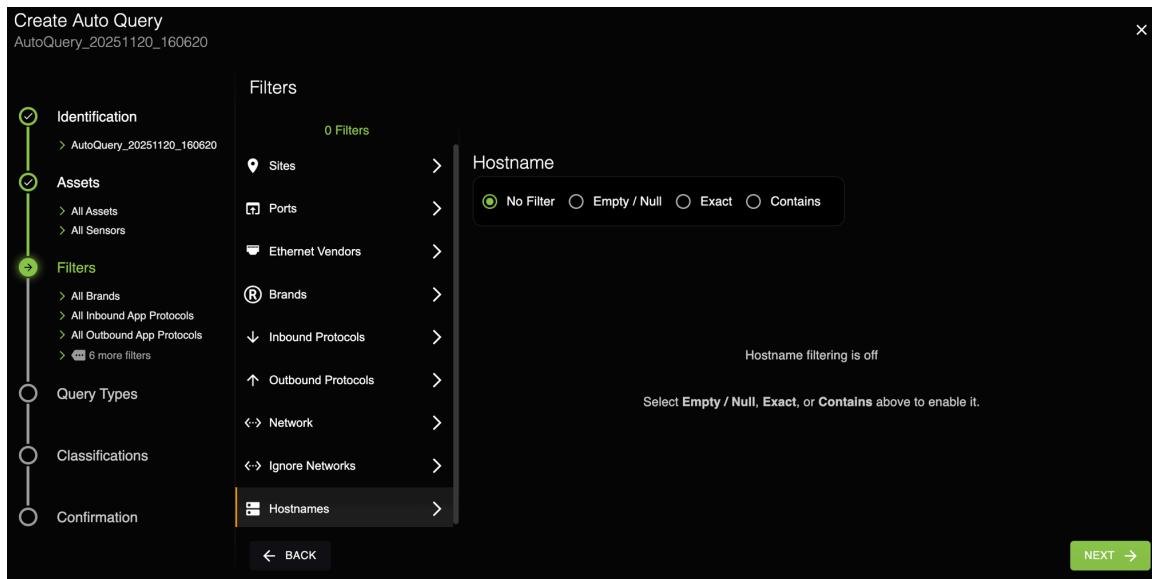
Note: The Ignore Networks filter allows you to select an IP range or individual IP addresses to ignore during the query.



- Hostnames

The Hostnames filter uses the hostname of the Asset and Targets the Asset based on the specified hostname information. To use this filter, select **No Filter** (default selection) or one of these options:

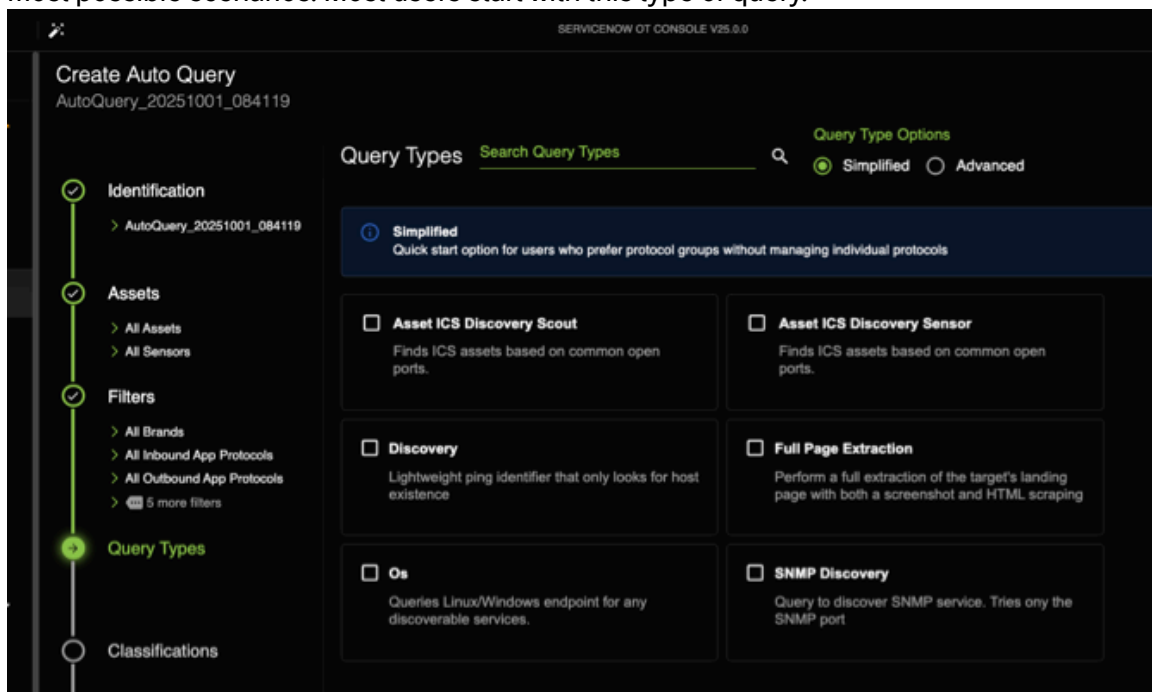
- **Empty/Null:** Queries Assets where the Hostname field is empty or null.
- **Exact:** Matches Assets whose Hostname equals any of the values you add. There is a field to type in a Hostname. All hostnames are included in this query unless you add at least one value.
- **Contains:** Matches Assets whose Hostname contains any of the substrings you add. There is a field for adding a value. All hostnames are included in this query unless you add at least one value.



9. Choose a filter and then select **Next**.

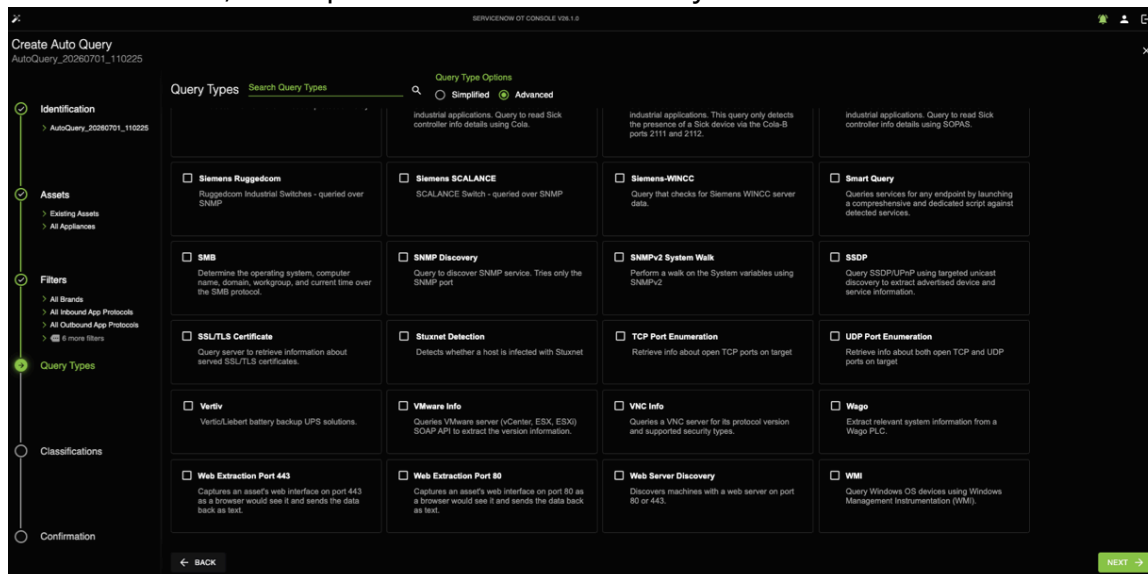
10. In the Query Types section, select the applicable query types as needed.

- The Simplified query types are a small list of easy-to-understand queries that should cover most possible scenarios. Most users start with this type of query.



Note: The simplified **Auto Query** type **Full Page Extraction** updates the query to perform a full extraction of your Target landing page. That means, this type of query includes both the screenshot and the HTML information.

- The Advanced query types are a list of all available advanced auto queries. As some of these queries can be riskier, require more technically complicated to understand, or specific to certain devices; these queries are recommended only for advanced users.



Some recently added Advanced Query types include but aren't limited to:

- MeISecQ** - Query the Mitsubishi MELSEC-Q Series
- Moxa** - Query to read the Moxa ICS setting
- IPC-UA Deep** - Retrieve info from an OPC-UA target
- ProfiNet DCE/RPC EPM** - Performs ProfiNet DCE/RPC EPM lookup requests
- ProfiNet DCP** - PLC protocol often used for communicating with Siemens devices; this protocol is newer than S7. NOTE: Since this is a layer 2 scan it may return more results than selected.
- SSL/TLS Certificate** - Query server to retrieve information about served SSL/TLS certificates
- WMI** - Query Windows OS devices using Windows

11. Optional: You can set up the Auto Query scan to include all open ports. To do this, select both or either the **UDP Port Enumeration** and / or **TCP Port Enumeration** (highlighted in the previous image) from the Advanced Query Types. Each scan determines all open ports for their two respective protocols.

Note: For these query types to be available, verify your ScanScripts.json driver is up to date; if not, upload the latest version of this driver. For information, see [Edit the Query Driver on Metadata tab](#).

12. Select Next

13. Optional: In the Classification section, select from the following.

Create Auto Query
AutoQuery_20260126_081930

Classifications

- ☐ **Brand based on MAC address**
assigns brand based on MAC address range match
- ☒ **Brand based on OCR words**
attempts to assign brand based on strings extracted by the OCR
- ☐ **Console Hostname Lookup**
attempts to determine an asset's hostname based on its IP address
- ☐ **Location**
sets a label and the location field with site name
- ☐ **Unknown**
marks the Asset brand and category to Unknown

← BACK NEXT →

- **Brand based on MAC address:** Assigns brand based on MAC address range match.
- **Brand based on OCR words:** Attempts to assign brands based on strings extracted by the OC. Fuzzy word search is supported.
- **Console Hostname Look up:** Attempts to determine an Asset's hostname based on its IP address.
- **Location:** Sets a label and the location field with Site name.
- **Unknown:** Marks the Asset brand and category Unknown.

14. Select Next.

15. In the Confirmation section, set the schedule, recursion, and duration.

Create Auto Query
AutoQuery_20261222_085541

Confirmation

Schedule

☐ Not Scheduled ☒ Scheduled

Day of the Week: Any Day

Time of Day: Any Time

Time Zone: (UTC-05:00) Eastern Time (New York)

Recursion

☐ Run Once ☒ Repeat

Every 7 Days

Duration

☐ Until Finished ☒ Window

For 4 Hours

← BACK NEXT →

16. Select **Next**.

17. Select the **Create Auto Query** button.

Result

The query is added to the Auto Query page.

Create an Auto Query ignore list

Create an Auto Query to exclude specified asset IP addresses from receiving scanning traffic.

Before you begin

Role required: admin

Procedure

1. Navigate to the Auto Query page.

2. Select the add icon .

3. In the Identification section, add the Auto Query name in the **Auto Query Name** field or use the generated name.

4. Select **Next**

5. In the Assets section, select the desired assets and targets.

The Assets section displays a choice of All Assets, New Assets Only, Incremental, Asset Discovery, and Asset Discovery & Query.

When the Query is set to use **All Assets**, then the Assets that are marked as ignored, are excluded from the list of targets.

The Targets section lists All Sensors, Specific Sensors, and Auto Targeting.

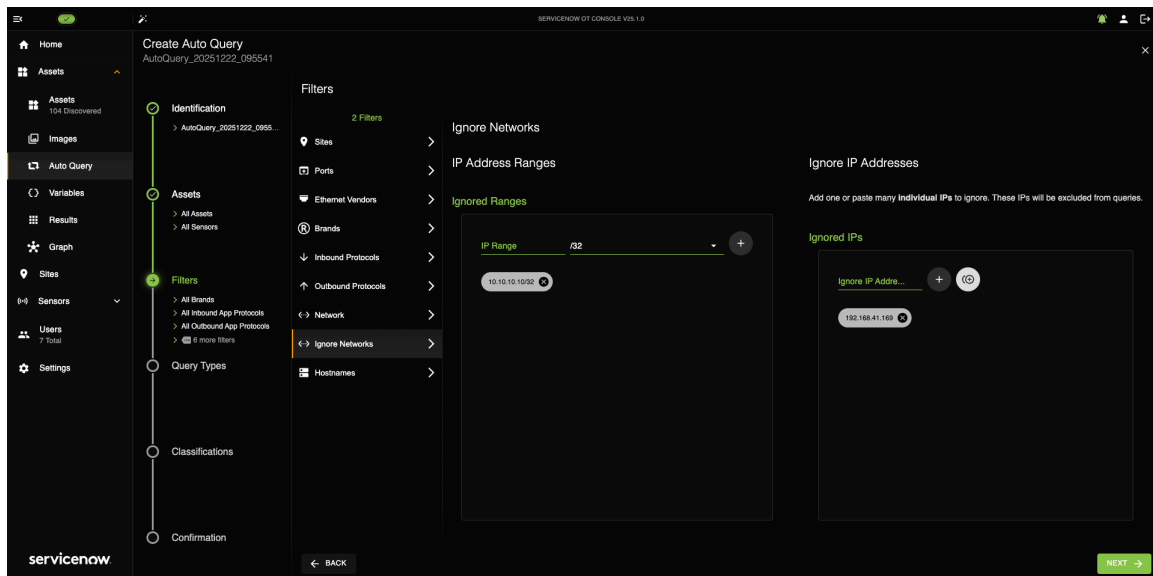
6. Select **Next**

7. Specify any filters in the Filters selection.

You can specify Sites, Ports, Ethernet Vendors, Brands, Inbound and Outbound Protocols, Networks, Ignore Networks, and Hostnames.

8. To create the ignore list, select the Ignore Networks filter.

- To ignore an IP Address Range, enter an IP Range in the IP Address Range section, and select the add icon .
- To ignore one individual IP address, enter an IP address in the Ignore IP Address section.
- To ignore multiple IP addresses, select the multiple selection icon  in the Ignore IP Address section, and use commas to separate the entries.



9. Select **Next**

10. In the Query Types section, select as many types needed from one or both the Simplified Query list or the Advanced Query list.

11. In the Classification section, if you choose to, you can select from the following.

- **Console Hostname Look up:** Attempts to determine an Asset's hostname based on its IP address.
- **Location:** Sets a label and the location field with Site name.
- **Unknown:** Marks the Asset brand and category Unknown.

12. Select **Next**

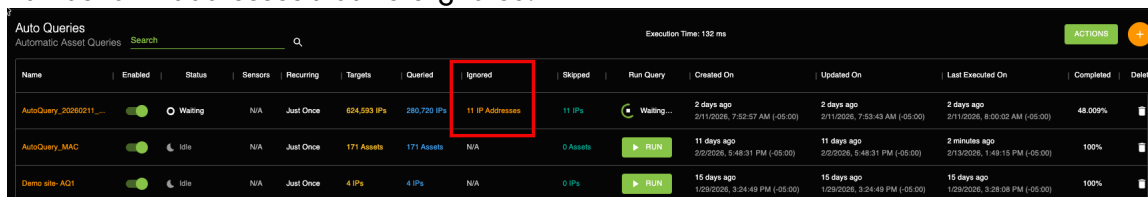
13. In the **Confirmation** section, set the schedule, recursion, and duration.



14. Select the **Create Auto Query** button to create the Auto Query ignore list.

Result

The Auto Query results are added to the Auto Query page. The **Ignored** column displays the number of IP addresses that were ignored.



Name	Enabled	Status	Sensors	Recurring	Targets	Queried	Ignored	Skipped	Run Query	Created On	Updated On	Last Executed On	Completed	Delete
AutoQuery_20251231_070936			N/A	Just Once	624,593 IPs	260,720 IPs	11 IP Addresses	11 IPs		2 days ago 2/11/2026, 7:52:57 AM (-05:00)	2 days ago 2/11/2026, 7:53:43 AM (-05:00)	2 days ago 2/11/2026, 8:00:02 AM (-05:00)	48.009%	
AutoQuery_MAC			N/A	Just Once	171 Assets	171 Assets	N/A	0 Assets		11 days ago 2/2/2026, 9:48:31 PM (-05:00)	11 days ago 2/2/2026, 9:48:31 PM (-05:00)	2 minutes ago 2/13/2026, 1:49:15 PM (-05:00)	100%	
Demo site-A21			N/A	Just Once	4 IPs	4 IPs	N/A	0 IPs		15 days ago 1/29/2026, 3:24:49 PM (-05:00)	15 days ago 1/29/2026, 3:24:49 PM (-05:00)	15 days ago 1/29/2026, 3:28:08 PM (-05:00)	100%	

Edit an Auto Query

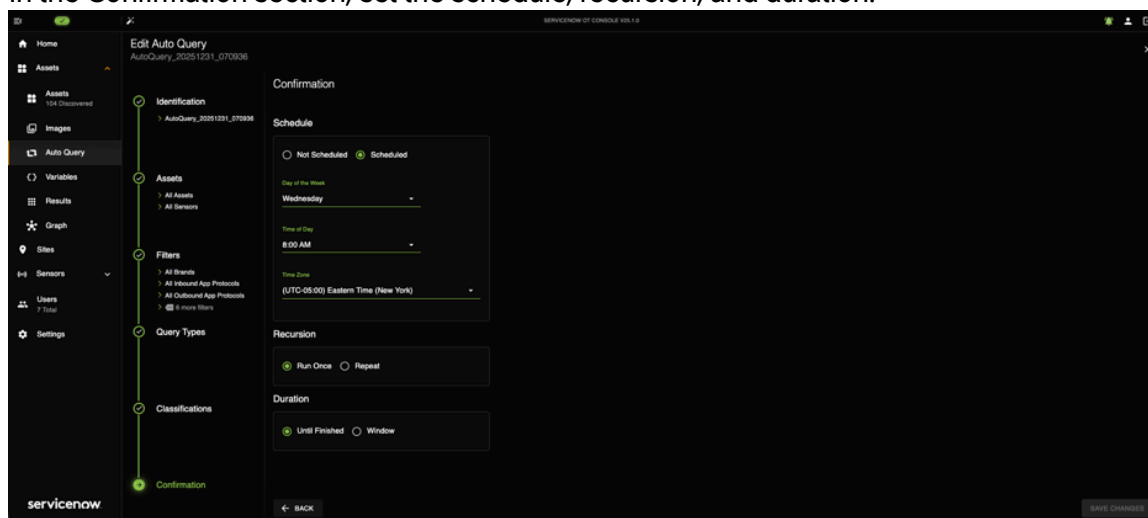
Edit an Auto Query to change or add parameters to your scan.

Before you begin

Role required: admin

Procedure

1. Navigate to the Auto Query page.
2. Select the query to be edited.
3. Step through each section in the Edit Auto Query view.
4. Change the settings that you want to change in the Assets, Filters, Query Types, and Classifications sections.
If needed, select the X icon in the right-hand corner of the screen to return to the Auto Query list and discard your changes.
5. In the Confirmation section, set the schedule, recursion, and duration.



Edit Auto Query
AutoQuery_20251231_070936

Identification
AutoQuery_20251231_070936

Assets
All Assets
All Sensors

Filters
All Brands
All Inbound App Protocols
All Outbound App Protocols
6 more filters

Query Types

Classifications

Confirmation

Schedule
☐ Not Scheduled ☒ Scheduled
Day of the Week: Wednesday
Time of Day: 8:00 AM
Time Zone: (UTC-05:00) Eastern Time (New York)

Recursion
☒ Run Once ☐ Repeat

Duration
☒ Until Finished ☐ Window

← BACK SAVE CHANGES

6. Select **Save** to save your changes or select **Cancel** to discard your changes

Create a Quick Scan

Create a **Quick Scan** from the Auto Query page.

Before you begin

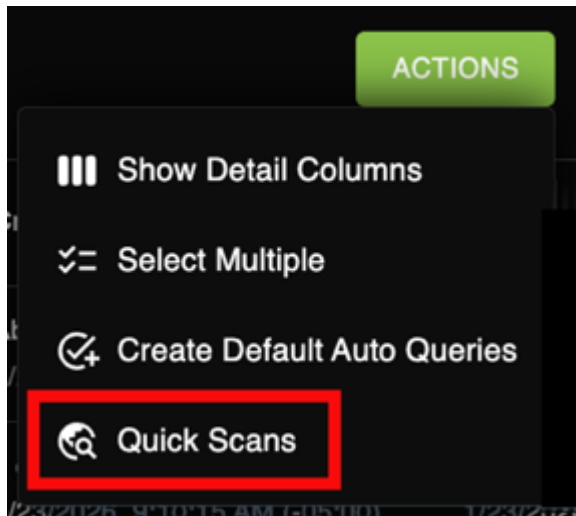
Role required: admin

About this task

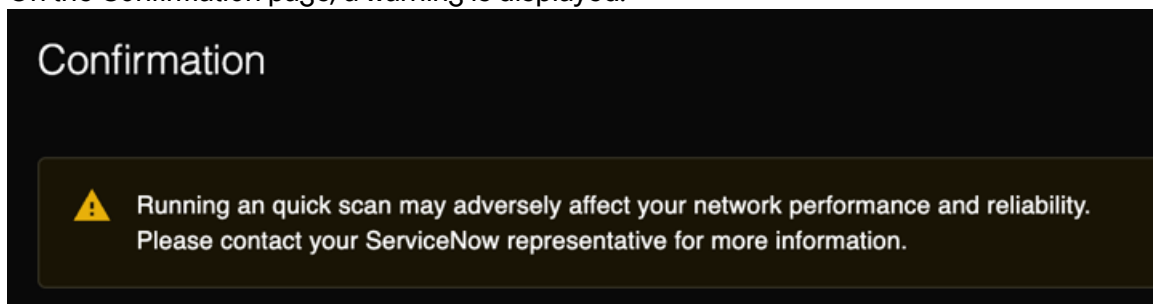
A Quick Scan has fewer options to choose from, but it also runs quickly at approximately 5 minutes. After the scan runs, select the View Results in the Results column.

Procedure

1. Navigate to the Auto Query page.
2. Select the **Action** button.



3. From the Action drop-down menu, select **Quick Scans**.
The Quick Scans page opens.
4. Select the add icon .
Fill in each step and then select the **Next** button to move to the next step.
5. In the **Identification** field, add a unique name or use the one provided.
6. From the available selections, select a **Target**.
Target selection includes:
 - **Assets**: You can select more than one and search for an Asset from the list.
 - **IP Addresses**: You can add one or more IP addresses to scan.
 - **IP Address Ranges**: Enter an IP Range. Select the add icon  to add additional IP ranges.
7. In the **Sensors** step, select the box next to one or more listed Sensors.
8. Select a **Scan Type**.
You can choose from the Simplified Query Type selection or toggle the **Advanced** button and select from the advanced query types. See the [Auto Query page](#) for additional information about Query Types.
9. On the Confirmation page, select the **Run Quick Scan** button to start the scan.
On the Confirmation page, a warning is displayed.



Variables

The Variables page provides a list of currently available variable sets.

Variable overview

The Variables page displays the available Variable sets on your system. It provides a Search Variables field above the variable list.

You can also create new variable sets. Variables are used for Auto Query scans and can be associated to a specific Site.

The columns on the page are:

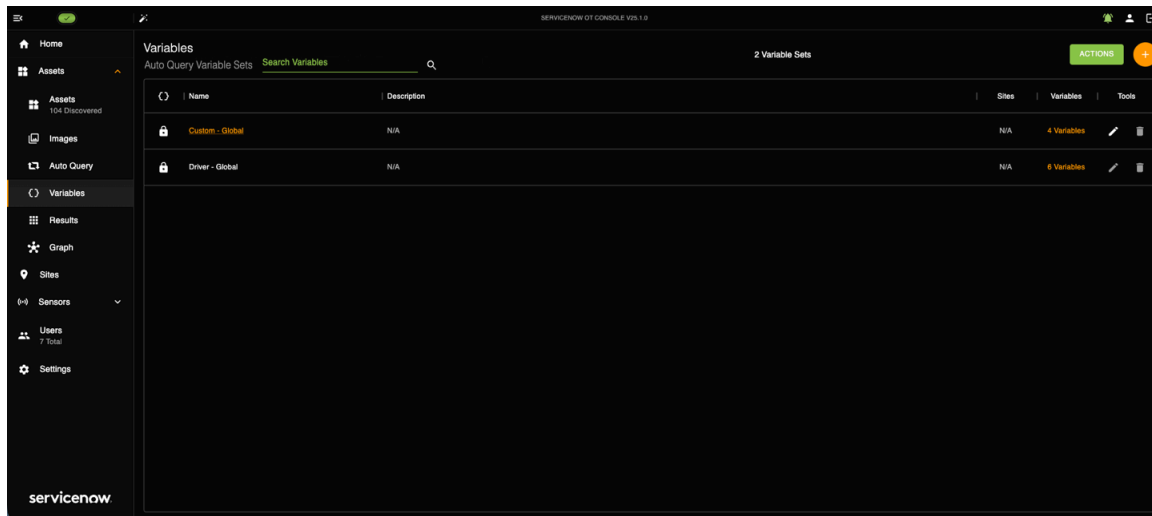
- The bracket dot icon  and lock icon  appear in the row next to the variable listing. When the bracket-dot symbol appears green next to the variable's name, the variable can be used for auto queries. When white, the variable can't be used for auto queries. The green lock indicates that the variable password is encrypted.

Note: Encrypted Variable values in Variable Sets are obscured.

- Name
- Description
- Sites display the name of the site to which the variable is associated.

Note: A Site can only be associated with a single Variable set, but a Variable set can contain many variables.

- Variables (number of variables)
- Tools
 - Select the pencil icon  to edit the variable set.
 - Select the trash can icon  to delete the variable set.

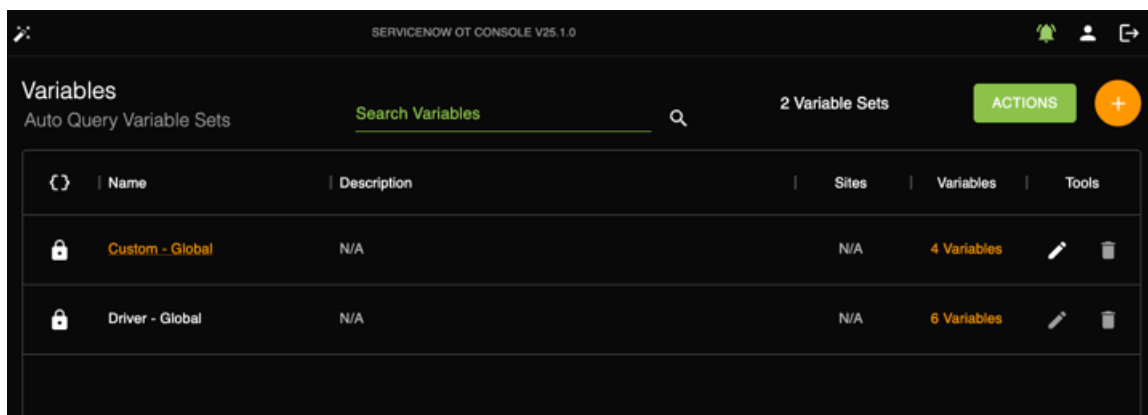


Special Variable sets

There are the following special variable sets:

- Custom - Global
- Driver - Global

The Custom-Global variable set can be edited by a user while the Driver - Global is read-only. The Custom - Global variable sets can be used to override indirectly the Driver - Global variable sets.



Name	Description	Sites	Variables	Tools
Custom - Global	N/A	N/A	4 Variables	[Edit] [Delete]
Driver - Global	N/A	N/A	6 Variables	[Edit] [Delete]

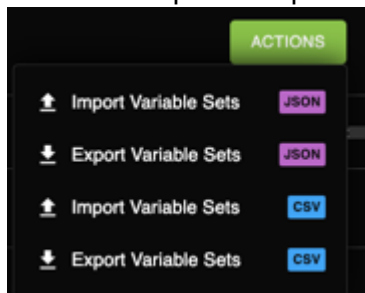
You can use variable sets (Custom - Global or Site-specific sets) to override a Variable set. See [Edit a Variable set](#) or [Create a Site-specific Variable set to use with Auto Query](#) for more information on editing a Variable set.

Query Behavior

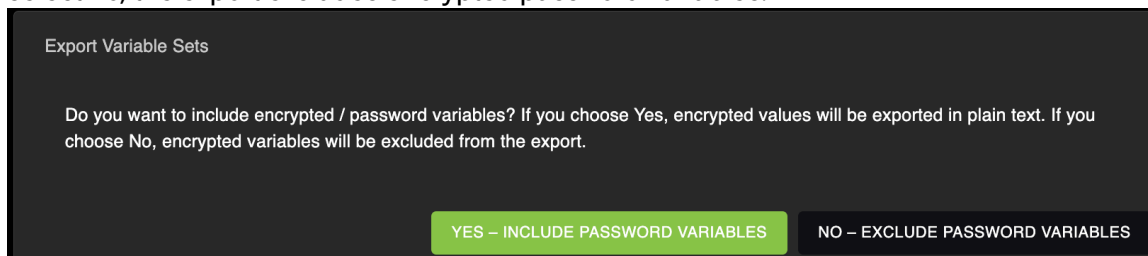
During a query, the query configuration is reviewed to see which Sites are being targeted. The query then searches to see if any Site-specific variable set override is defined. If no override is defined, it then searches to see if any Custom - Global override is defined. If it doesn't find a custom override, the query uses the default variable set from the Driver - Global.

Importing or exporting Variables sets

You can import or export variable sets. You can select either the JSON or CSV formats. Select **Actions** to import or export.



When you export Variable sets in either JSON or CSV format, you're prompted to include encrypted password variables. If you select yes, the values are exported as plain text. If you select no, the export excludes encrypted password variables.



Export Variable Sets

Do you want to include encrypted / password variables? If you choose Yes, encrypted values will be exported in plain text. If you choose No, encrypted variables will be excluded from the export.

YES - INCLUDE PASSWORD VARIABLES NO - EXCLUDE PASSWORD VARIABLES

If the encrypted password is exported as plain text, it is no longer hidden and secure.

Note: Encrypted Variable values in Variable Sets are obscured. Encrypted values display as dots when set to encrypted.



The screenshot shows the 'Variables' table in the ServiceNow interface. The table has columns for Name, Value, and Note. The 'Value' column for 'snmp_communities' and 'dns_servers' is obscured with dots, indicating encrypted values. The 'Note' column for all entries is 'N/A'. There are edit and delete icons for each row. An orange '+' icon is in the top right corner of the table header.

Name	Value	Note
snmp_communities		N/A
dns_servers		N/A
flexidome_usernames		N/A
flexidome_passwords		N/A

Note: For information on creating a Site-specific Variable set, refer to [Create a Site-specific Variable set](#).

Create a Variable set

Create a Variable set for an Auto Query scan created in the Discovery Console for OT.

Before you begin

Role required: admin

Procedure

- 1. In the Console, navigate to **Assets > Variables**.
- 2. Select the add icon .

3. On the **Create Variable Set** page, add the necessary information and then completion, select **Next**.

4. **Identification:** Enter information in the fields for the Variable name and description.

5. **Site:** In the Select Sites section, put a check mark in the box next to a site name (if available).

Using the icons under the list allows you to select all  or deselect all sites .

6. **Variable:** Select from the list of available Variables.

7. **Confirmation:** Confirm to create the Variable.

Result

The new variable appears in the Variable list.

Note: A Site can only be associated with a single Variable set, but a Variable set can contain many variables.

Edit a Variable set

Edit a Variable set for an Auto Query scan created in the Discovery Console for OT.

Before you begin

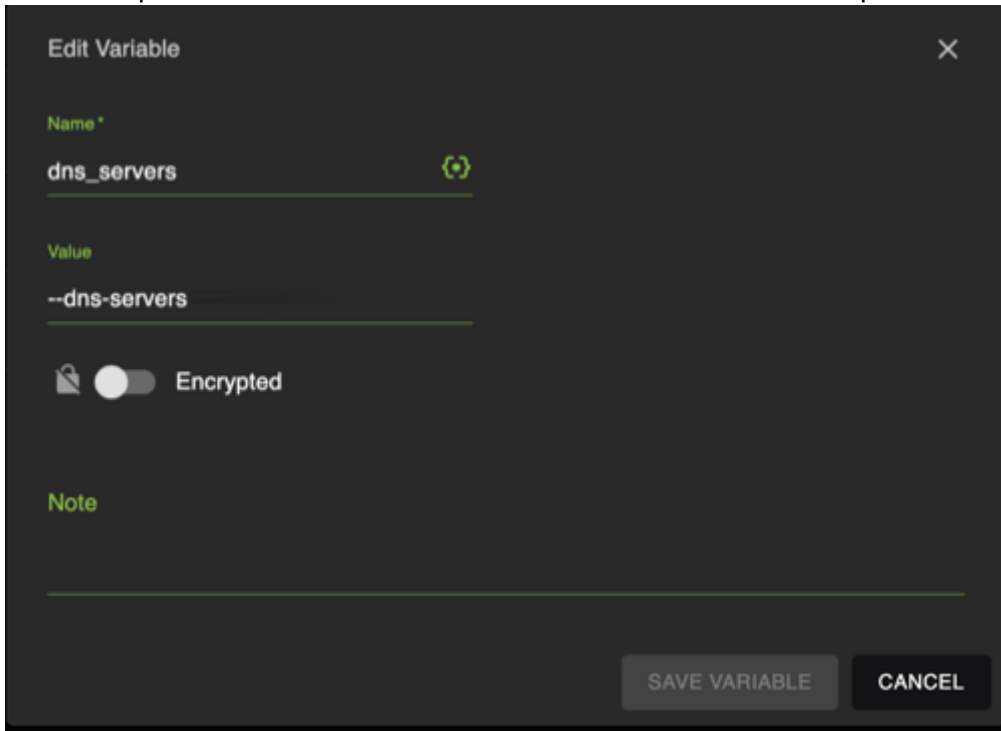
Role required: admin

Procedure

1. Navigate to the Variables page.
2. Select a Variable set.

Note: Editing the Custom - Global variable set allows you to globally override variable values defined in the Driver - Global variable set.

3. Select the pencil icon  for the Variable.
The Edit Variable Set view opens.
4. Edit parameters as needed.
 - a. **Identification:** Edit the name and description of the Variable.
 - b. **Sites:** Select a different site from the original selection if needed.
5. In the Variables section, you can edit or delete the variables as needed.
Select the pencil icon to edit the Variable. The Edit Variable window opens.



The screenshot shows the 'Edit Variable' dialog box. It has a title bar with 'Edit Variable' and a close button. The main content area includes:

- Name ***: A text field containing 'dns_servers' with a refresh icon to its right.
- Value**: A text field containing '--dns-servers'.
- Encrypted**: A toggle switch that is currently turned off, with the label 'Encrypted' to its right.
- Note**: A text area for additional notes.

At the bottom of the dialog are two buttons: 'SAVE VARIABLE' and 'CANCEL'.

6. To hide the value of a Variable, slide the toggle next to Encrypted.

Note: Encrypted Variable values in Variable Sets are obscured. Encrypted values display as dots when set to encrypted.

Name	Value	Note
snmp_communities		N/A
dns_servers		N/A
flexidome_usernames		N/A
flexidome_passwords		N/A

Create a Site-specific Variable set to use with Auto Query

Create a Site-specific Variable set for use in Auto Queries.

Before you begin

Role required: admin

About this task

Create a Site-specific Variable set to define query Variable values for use in Auto Queries. You can use the Variable set as a credential for your Site.

Note: A Site can be associated to only one Variable.

Procedure

1. Navigate to the Variable page in the Console.
2. Create a Variable as described in [Create a Variable set](#).
3. When you create the variable, select a Site to associate it.
4. Create an Auto Query as described in [Create an Auto Query](#).
5. In the Filter section of the query, select the Sites filter.
6. From the list of sites, select the site to associate to your variable.
7. Complete creating the query.
8. Run the Auto Query that you created.

Result

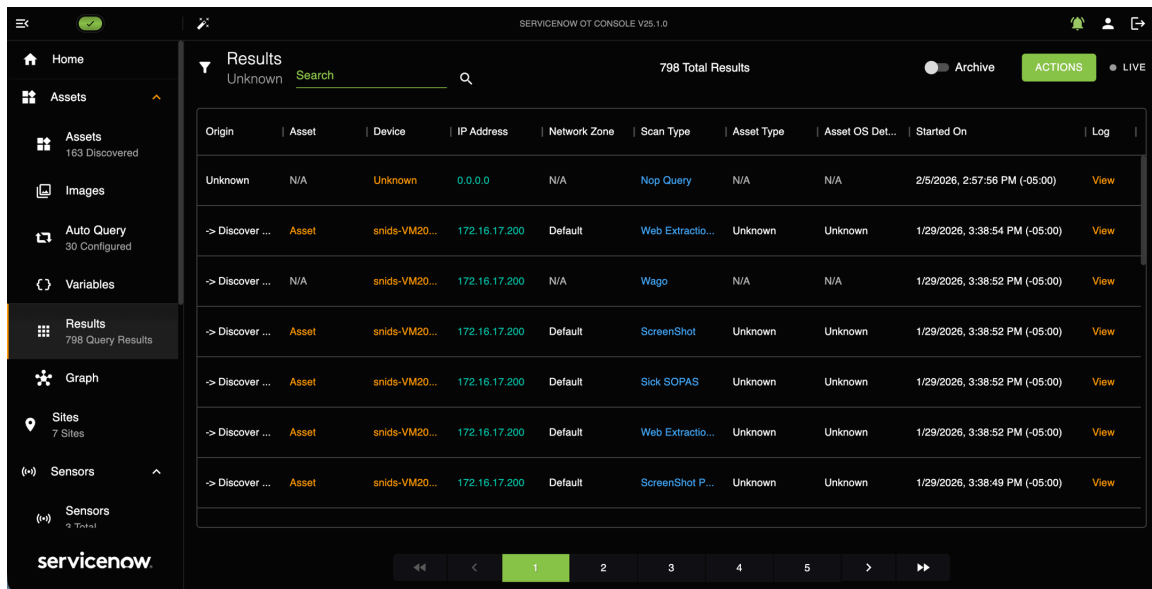
Your Site is queried and associated to the Variable.

Results page

The Results page provides the results from your queries in the Discovery Console for OT.

The Results page contains a list with all the scan results in the system. Each scan is displayed along with the associated Device, IP Address, Network Zone, Scan Type, Asset Type, Asset OS Details, Started On, and Log. The following image shows an example of the Results page.

Note: You can't export RAW XML results if your Console license is invalid (absent or expired).

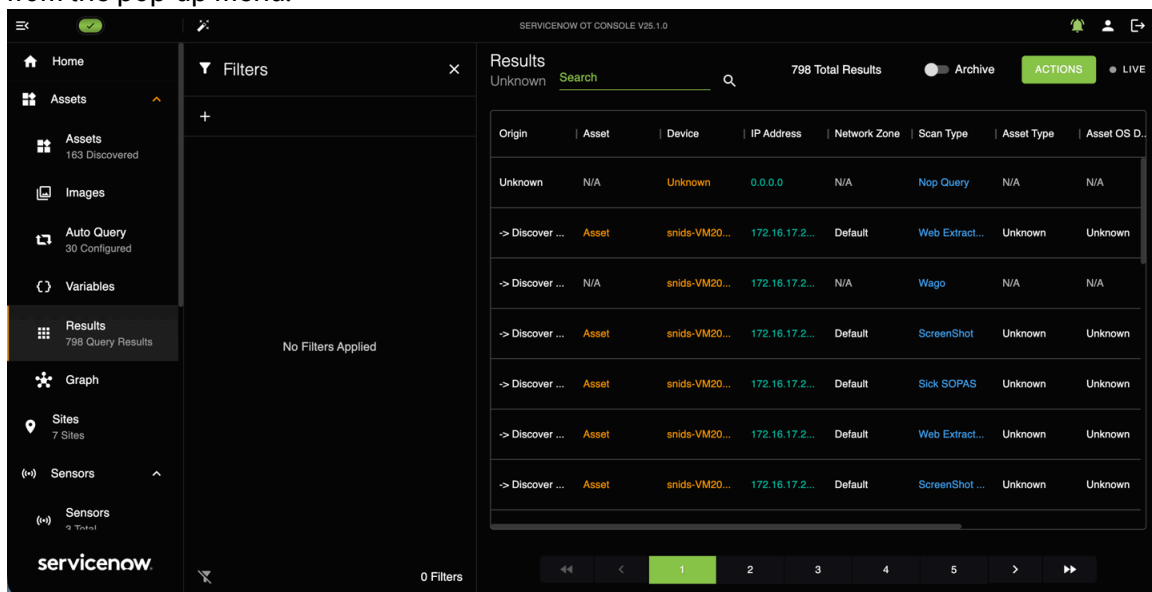


To access the Results page, navigate to **Assets > Results**.

To find a specific scan, you can enter text into the Search bar on the top of the page under the Results heading.

Result filters

Use the filter panel to select which queries display in the results list. To filter the scan results, select the Add Filter icon **+** in the filter panel. Put your cursor in the filter field and select a filter from the pop-up menu.



See [Filter results](#) for more information.

Viewing results

On the Results page, you can view details of a result by selecting column entries.

Asset

Selecting an asset name in the Asset column opens the asset editing window. This view has three tabs, Details, Image, and Module On the Details tab you see

Identification, Classification, Timeline, and other detailed sections. You can select Edit if you need to change any of these settings. If there is an image attached, it displays in the Detail and Images tabs. The Modules tab displays specific information about system modules, such as if the asset is a CPU or PLC, and the manufacturer's name.

Appliance

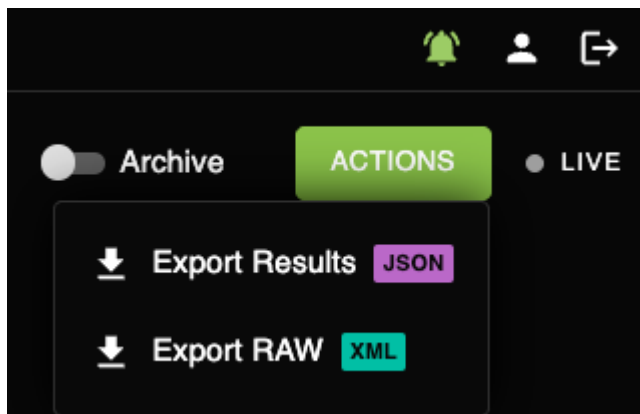
The Appliance column lists the name of the Sensor or Collector used during the query. Selecting the name from this column allows you to edit the query appliance's information and configuration.

Log

Select View in the Log column and the query log displays. You can copy the log for later use and for troubleshooting.

Action button

The Results page **Action** button lets you export the scan results. You can **Export Results** in JSON format or **Export RAW** in XML format.



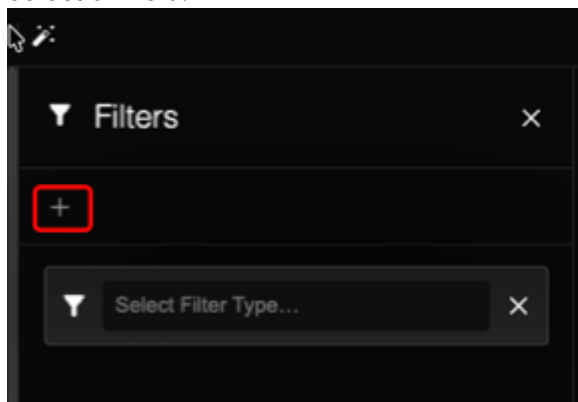
The RAW data format is useful for debugging and verification.

Filter results

The Results page provides a filter to find specific types of queries of information.

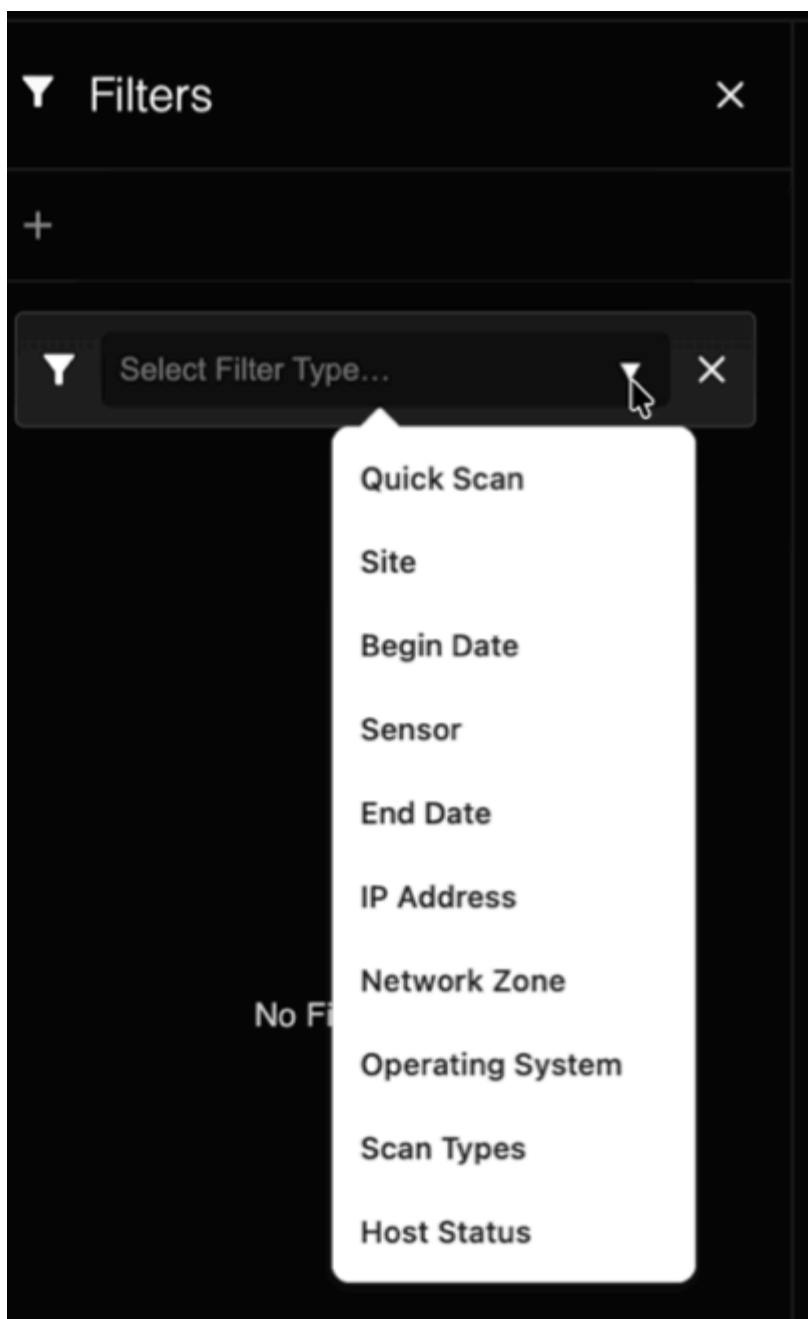
Filtering the query results

Much like the Assets page, the Results page provides a filter to the left of the Results list. To open the Filter type list, select the plus sign **+** under the Filter header. This opens the drop-down selection field.

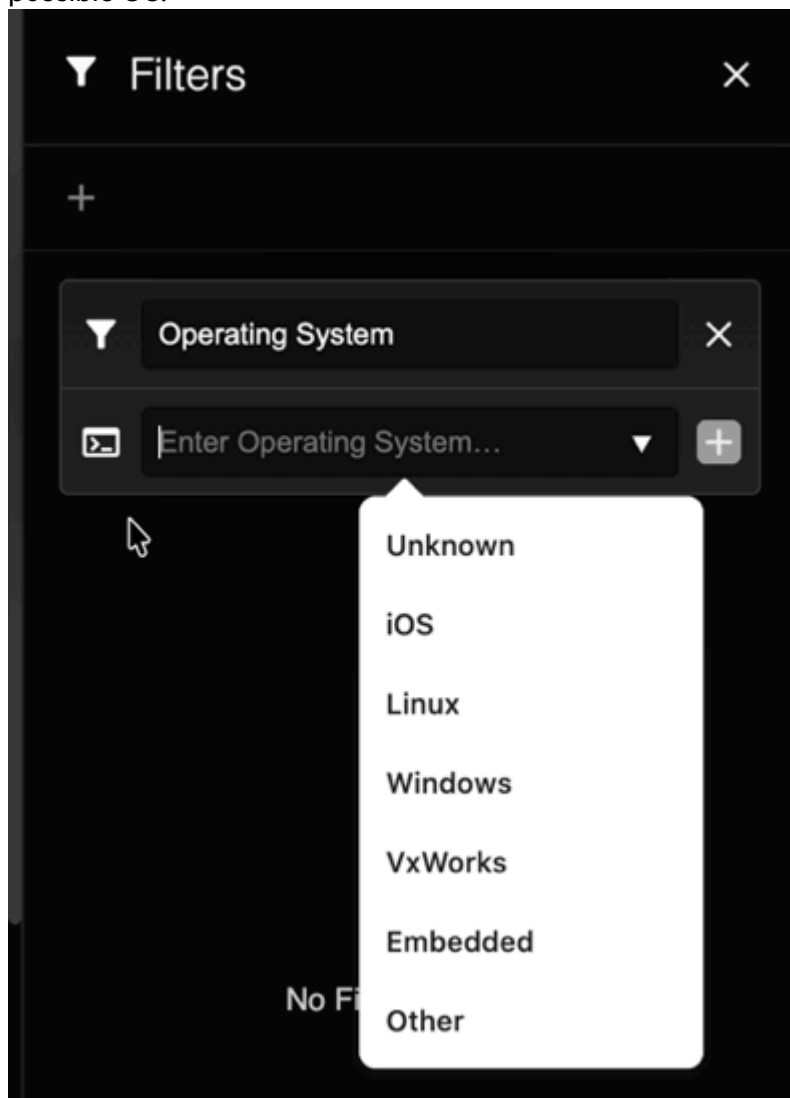


The menu drops down and you can select from the following list.

- Quick Scan
- Site
- Begin Date
- Sensor
- End Date
- IP Address
- Network Zone
- Operating System
- Scan Types
- Host Status



If you select Operating System, for example, another drop-down menu opens with a list of possible OS.



After you have made your selection, any query that matches the filter displays on the Result page.

Filter results for Host Status

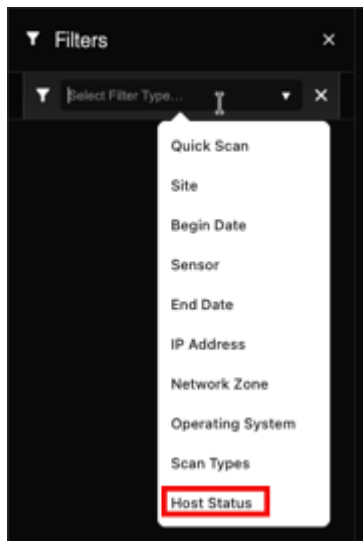
Filter your query results by Host Status. Verify whether devices were reachable when the query was executed.

Before you begin

Role required: admin

About this task

In the Scan Results filtering types, the **Host Status** enables users to view query results based on whether the queried host was **Up** or **Down**. This filter is derived from the **Nmap XML status field** inside the Raw scan output.



Note: This filter is based on raw scan output and does not depend on scan type. If a scan output does not contain a host status `state= "up | down "` field, it does not match the Host Status filter.

Using the Host Status filter helps to quickly narrow results such as:

- Shows only reachable devices (Up) to review open ports or services.
- Shows only unreachable devices (Down) to troubleshoot network issues, firewall rules, wrong IPs, or powered-off devices.

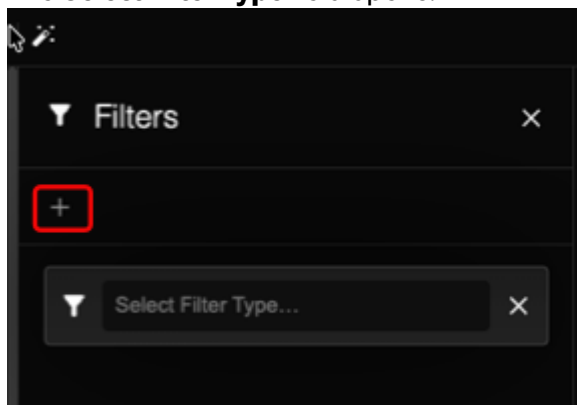
Raw data is useful for debugging and verification because:

- Reason field: Raw data confirms why a host was marked Up/Down.
- Good for investigation: Raw data shows what the Nmap actually returned.
- Script validation: Raw data helps validate scripts when scan parsing or mapping doesn't show expected information.

Procedure

1. Navigate to the Results page.

2. In the Filter panel, select the plus icon. 
The **Select Filter Type** field opens.

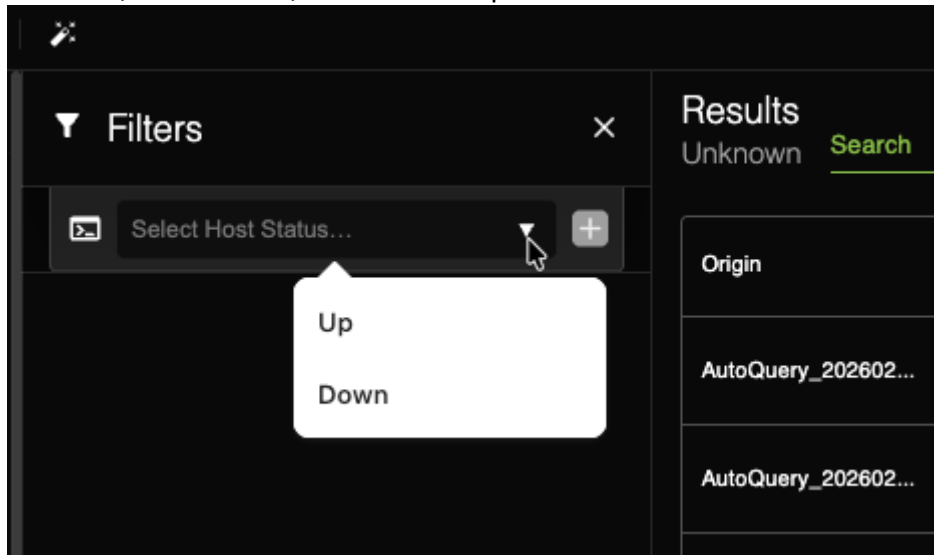


3. In the Filter field, select Host Status from the drop-down menu.
The **Select Host Status** field opens.

4. Select from the pop-up choices one of the following.

Note: **Up/Down** in this instance means the **host status from the scan result (Nmap)** for that IP during that query run.

- **Up** means the target asset responded, that is, the appliance was able to reach it and also got a response back.
- **Down** means the target asset did not respond; this could mean it is offline, blocked by firewall, unreachable, or it did not respond.



5. Using the Host Status filter helps to quickly narrow results:

- Showing only **reachable assets** (Up) to review open ports/services.
- Showing only **unreachable assets** (Down) to troubleshoot network issues, firewall rules, wrong IPs, or powered-off devices.

6. Raw data is useful for debugging and verification because:

- Raw data confirms why a host was marked Up/Down (reason field).
- Raw data shows what Nmap actually returned (good for support/investigations).
- Raw data helps validate scripts when querying/mapping doesn't show expected information.

Appliances page

The Appliances page displays active appliances in the Discovery Console for OT.

Appliances

The Appliances page displays the current Sensors and Collectors that have run or are running your queries. The information displayed includes the following:

- Name
- Type
- Endpoint
- Status
- Queue

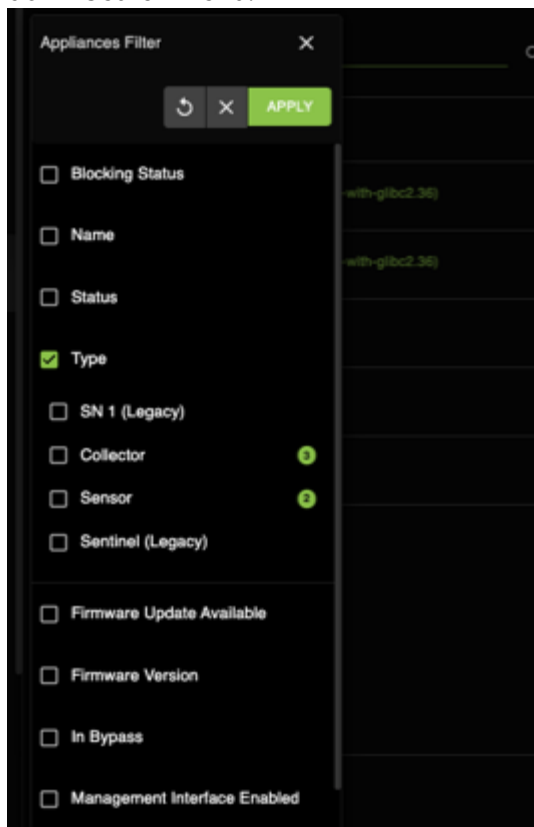
- CPU
- Configuration Status
- Update Available?

Name	Type	Endpoint	Status	Queue	CPU	Configuration Status	Update Availabl...
snids-VMtest	Sensor	Mgmt: 192.168.40.93	Connection Lost		N/A		NO
Win-b1d218ff (Windows-10.0.19045-SP0)	Collector	Mgmt: 192.168.41.167	Connection Lost		N/A		NO
Lin-a12bcc2b (Linux-6.1.0-11-amd64-x86_64-w	Collector	Mgmt: 192.168.40.73	Powered On		N/A		NO
Lin-eb6433c2 (Linux-4.18.0-553.el8_10.x86_64	Collector	Mgmt: 192.168.40.64	Powered On		N/A		NO
snids-onlogic250	Sensor	Mgmt: 192.168.41.109	Powered On		N/A		NO
TaraUITestSensor	Sensor	Mgmt: 192.168.41.170	Powered On		N/A		NO

For more information, see [Edit an Appliance](#).

Search by type

You can search for a type of appliance by entering the type in the Search field. Or you can open the Filter and select by the available labels. For example, if you want to view just the Collectors, you can type Collector in the Search field. You can also check the box next to Type in the drop-down Search menu.



Then choose Collector. The Appliances list now shows only the current Collectors.

Name	Type	Endpoint	Status	Queue	CPU	Configuration Status	Update Availabl...
Lin-99d8e75e (Linux-6.1.0-39-amd64-x86_64-with-glibc2.36)	Collector	Mgmt: 192.168.40.82	Connection Lost	N/A	N/A		NO
Lin-9b9e0e48 (Linux-6.1.0-39-amd64-x86_64-with-glibc2.36)	Collector	Mgmt: 192.168.40.82	Connection Lost	N/A	N/A		NO
Win-9fd47f57 (Windows-10-10.0.26100-SP0)	Collector	Mgmt: 192.168.40.70	Connection Lost	N/A	N/A		NO

Using Appliances in Queries

The Discovery Sensor for OT executes the query to discovery assets and creates the OT environment inventory. The OT Discovery Collector is used to discover assets within segments of the OT network where a Sensor can't reach. It is deployed deep within the network zones in your OT environment.

When you create an Auto Query in the Console, you can choose specific Appliances in the Assets section. When choosing Assets for the query, you can assign the Target to all appliances, specific appliances, or auto targeting. If you select **Specific Appliances**, you can select the appliances you want from a provided list. One restriction is that you must select at least one Sensor from the list as

Create Auto Query
AutoQuery_20260610_103351

Assets

Assets to Query

- ☒ Existing Assets
- ☐ New Assets Only
- ☐ Incremental
- ☐ Asset Discovery
- ☐ Asset Discovery & Query

Targeted Appliances

- ☒ All Appliances
- ☐ Specific Appliances
- ☐ Auto Targeting

← BACK NEXT →

well.

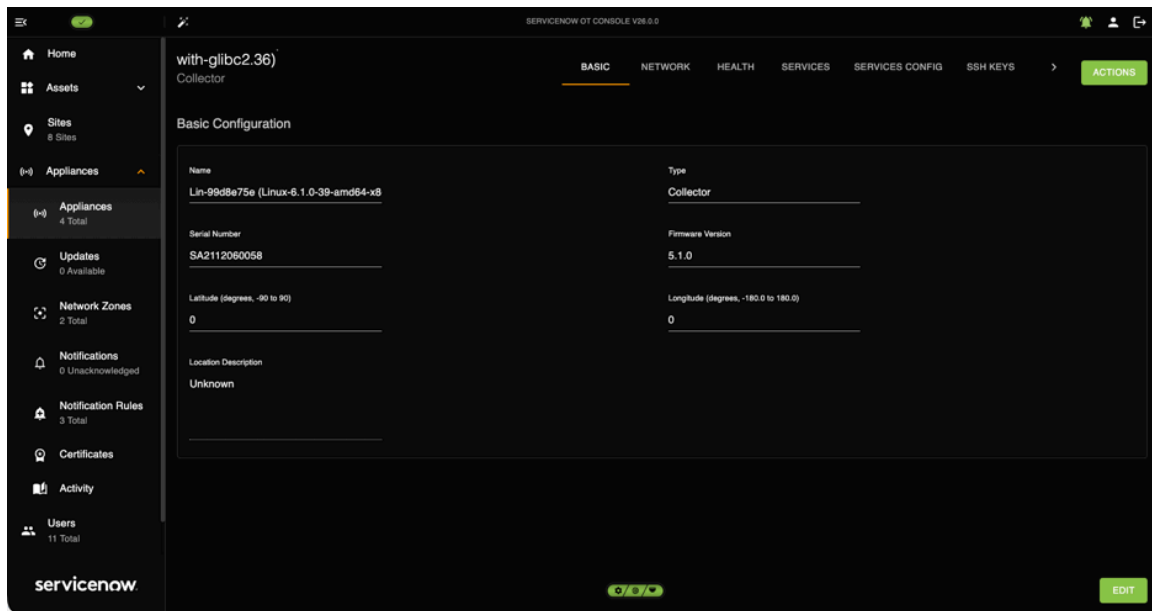
For more information, see [Auto Query page](#) and [Create an Auto Query](#).

Edit an Appliance

This section describes what information that is available and that is setup on an Appliance record

Edit an Appliance

To edit any appliance, select the Name of the appliance. The appliance record opens.



The appliance view has tabs with additional information and options. Move to a tab and then select the **Edit** button to edit any of the appliance settings. Select the **Save** button to save your changes or **Cancel** to discard them.

The following sections describe the available appliance information shown as tabs in the record.

Basic

This tab displays the basic configuration information for the appliance. The configuration includes the **Name**, **Type**, **Serial Number**, and **Firmware Version**. It also contains user-definable location information including fields for **Latitude**, **Longitude**, and **Location Description**.

Network

The **Network** tab shows the network settings as they're currently configured for the appliance. Each field is described in the following list:

- **Console Endpoint:** Shows the IP address of the Discovery Console for OT that the appliance is configured to use.
- **Appliance Gateway:** Shows the IP address assigned to the appliance that is used to route traffic between networks.
- **Management Interface:** Connects the appliance to an out-of-band network for communication with the Discovery Console for OT.
 - **Management Endpoint:** Sets the IP address for the Sensor which it uses to communicate with the Discovery Console for OT.
 - **Management Subnet:** Sets the subnet mask/Classless Inter-Domain Routing (CIDR) for the appliance communication with the Discovery Console for OT.
 - (Optional) **Management VLAN:** Specifies the VLAN identifier that the management interface uses to tag network communications for participation in VLAN segregated networks.
- **Span Interface:** When enabled, allows the appliance to collect all network traffic received on the ETHERNET 1 port. This allows the IDS to collect data from the network. When disabled, the appliance can't perform any data collection.
- **Networks Monitored by Arpwatch:** Lists networks that are being monitored by Arpwatch.
- **Ethernet Interfaces:** Lists all Ethernet Interfaces for the appliance. The list includes the Interface name and the MAC Address for each one.

Health

The **Health** tab enables you to view graphs reflecting trends in CPU, memory, disk utilization, and temperature and network input and output over time. You can set the data and time you want the CPU activity to reflect.

Services

You can configure specific services that run on an appliance. Currently, you can use this feature to enable or disable the SSH service on an appliance. Select the **Edit** button and then select the toggle to turn the SSH service on or off. This setting provides the **Status** and **Updated On** fields for the SSH service. Similarly, you can enable or disable the Log Streaming and Web Management services and view the corresponding **Status** and **Updated On** fields. The SSH service is enabled by default on all Sensors to facilitate post-installation configuration.

Services Config

The **Services Config** tab includes the **Log Streaming Service**, and the **Web Management Service**. You can use the Log Streaming Service to stream logs from appliances to the Discovery Console for OT. This service also retains logged information for a longer period, which can assist in quicker customer issue resolution.

To set the **Syslog Severity Level** for the Log Streaming Service, select **Edit** and use the drop-down menu to select the severity. You can select the minimum log severity, Informational, to include in the streaming for the appliance. Selecting the Debug level results in the most information being logged.

The data stream isn't viewable in the Console UI. The Console only provides the ability to enable or disable the service and set the log severity level. Streamed log information is retained on the Console for 30 days.

You can use the Web Management feature to reset the Web Management Service password on the appliance. To reset the password, select **Edit**. Enter a password in the **Password** field, enter the same password in the **Confirm Password** field, and then select **Save**. The **Status** and **Updated On** fields provide information about the Web Management Service on the appliance.

SSH Keys

On this tab, you can add public keys by listing the SSH key name in the **SSH Key Name (Optional)** field. You can also select **Paste SSH key(s) - one per line** and paste in keys. **Password Authentication** is enabled by default in the initial appliance install. To enable or disable the SSH password authentication, slide the toggle. You can also upload your own SSH Keys. The required format for a key is .pub.

Duplicate keys are automatically removed, so the same SSH key appears only once, even with small formatting differences like extra spaces.

Note: As a safety feature that allows continued SSH access, disable **Password Authentication** only if you have uploaded at least one SSH public key to the appliance.

The screenshot shows the 'SSH Keys & Access' configuration page for a collector named 'glibc2.36'. The page has a dark theme. At the top, there's a navigation bar with tabs: BASIC, NETWORK, HEALTH, SERVICES, SERVICES CONFIG, SSH KEYS (selected), and SITES. An 'ACTIONS' button is on the right. Below the navigation bar, there's a section titled 'SSH Keys & Access' with a toggle for 'Password Authentication' which is turned on. The main content area is divided into two columns. The left column is titled 'Add Public Key' and contains a text area for 'SSH Key Name (Optional)'. Below that is a section 'Paste SSH Keys' with a blue box containing instructions: 'Paste one or more SSH sshKeys below, with one key per line. Each line should be formatted as follows: {format} {public_key} {credentials}. Example: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAA... username@hostname'. Below the instructions is a text area labeled 'Paste SSH key(s) - one per line' and an 'ADD KEY' button. The right column is titled 'Upload SSH Keys' and contains a blue box with the instruction: 'Upload one or more SSH public keys for this sensor in .pub format'. Below this is an 'UPLOAD SSH KEY(S)' button.

Sites

The **Sites** tab displays which sites are associated with the selected appliance record during an Auto Query. The Allow/Deny setting indicates whether the appliance is associated with a listed Site. The tab also displays the site name, recommended setting for that site, and the reason for the recommendation. A Deny recommendation means the Site does not appear to be related to the appliance. An Allow recommendation means the Site's network ranges match the Device IP. Select the **Edit** button to change the Allow/Deny settings. Select the **Save Associations** button to save changes or **Cancel** to discard any changes.

The screenshot shows the 'Sites' configuration page for the same collector 'glibc2.36'. The navigation bar is the same, but the 'SITES' tab is selected. Below the navigation bar, there's a section titled 'Sites' with a subtitle 'Associated with Appliance'. To the right of this subtitle, it says '8 Available Sites, 6 Associated Sites'. The main content area is a table with columns: Site Name, Allow, Deny, Recommend, and Reason. The table lists 8 sites. The first two sites, 'Auckland' and 'Console Generated Site 4ea9ea4f', are associated with the appliance (indicated by a green checkmark in the 'Allow' column). The other six sites are not associated (indicated by a red 'X' in the 'Deny' column). The 'Recommend' column shows 'Deny' for all sites except 'Console Generated Site 4ea9ea4f', which is 'Allow'. The 'Reason' column provides the rationale for each recommendation.

Site Name	Allow	Deny	Recommend	Reason
Auckland	☒	☐	Deny	Site appears to be unrelated to this sensor.
Console Generated Site 4ea9ea4f	☒	☐	Allow	Site's network ranges match Device IP.
Demo Site- Console	☐	☒	Deny	Site appears to be unrelated to this sensor.
Home base	☐	☒	Deny	Site appears to be unrelated to this sensor.
Leesburg	☐	☒	Deny	Site appears to be unrelated to this sensor.
New12312025	☒	☐	Deny	Site appears to be unrelated to this sensor.
Oulu	☒	☐	Deny	Site appears to be unrelated to this sensor.
Test Site	☐	☒	Deny	Site appears to be unrelated to this sensor.

An 'EDIT' button is located at the bottom right of the table.

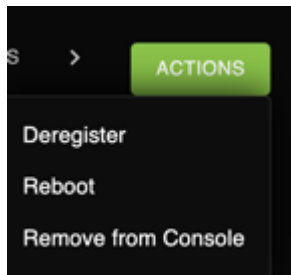
Status

This tab shows the current connection status of the appliance, including deployment status for basic configuration, network configuration, arpswatch networks configuration, policy, and firmware updates. Editing these settings is not available.

Actions button

The **Actions** button in the appliance record enables the following actions.

- **Deregister Device:** Deregisters the appliance from the Console. This action resets the network settings to factory defaults and removes the appliance from the Console.
- **Reboot Device:** Reboots the appliance.
- **Remove from Console:** Removes the appliance from the Console.



Sites page

A Site represents a physical location in your organization, such as a DATACENTER, office, or IoT site. Each Site includes location details, time zone settings, and network range configurations that determine which IP addresses the Console for scans during discovery.

- i Note:** Sites is the starting step to group assets. All devices that are part of a given network range defined in the Site configuration are assigned to that site. If there are multiple Network Zones within the Site, these zones could be assigned to a Site for grouping purposes.

The Sites page contains a list of all the sites available in your Discovery Console for OT system. For each site, you can view the network range, time zone, latitude, and longitude. The following image shows an example of the Sites page.

Name	Network Ranges	Time Zone	Latitude	Longitude	Edit	Delete
Ashburn	1 Network Range	America/New_York	36.8577733691	-77.6381081357		
Charlottesville	7 Network Ranges	America/New_York	38.0378509290	-78.4666714262		
Houston	5 Network Ranges	America/Chicago	29.7615009144	-95.3503449059		

Note: You can't select the same IP Addresses for both the Include and Ignore selections for the Site without triggering an error.

Add a Site

Add a site to your Discovery Console for OT.

Before you begin

Role required: admin

Procedure

1. Navigate to the Sites page.

2. Select the add icon .
The Site creation wizard opens.

3. In the Identification section, enter a unique name for your site.

Note: The site name must be unique across your Discovery Console instance. Use a descriptive name that clearly identifies the location. For example, "Seattle_DataCenter" or "NYC_Office_Building_A".

4. Select **Next**.

5. In the Address section, add the physical address to your site.
This information helps identify the site's geographic location for organizational purposes.

6. Select **Next**.

7. In the Location section, specify the geographic coordinates using one of these methods:

- Enter the latitude and longitude coordinates directly in the provided fields.
- Select a location on the interactive map to automatically populate the coordinates.

8. Select **Next**.

9. In the Time Zone section, begin entering the zone name in the Search field to quickly filter available time zones.

The Search filter displays all related Time Zones on the page.

10. Select the button next to the desired Time Zone, and then select **Next**.

11. In the **Network Ranges** option, select at least one range or a Network Zone that has at least one range.

The Network Ranges configuration determines which IP addresses Discovery Console scans (including) and which it ignores during discovery operations for this site.

12. Add IP address ranges to scan:

a. Under Include, select the **Begin IP** field and select or enter the starting IP address.

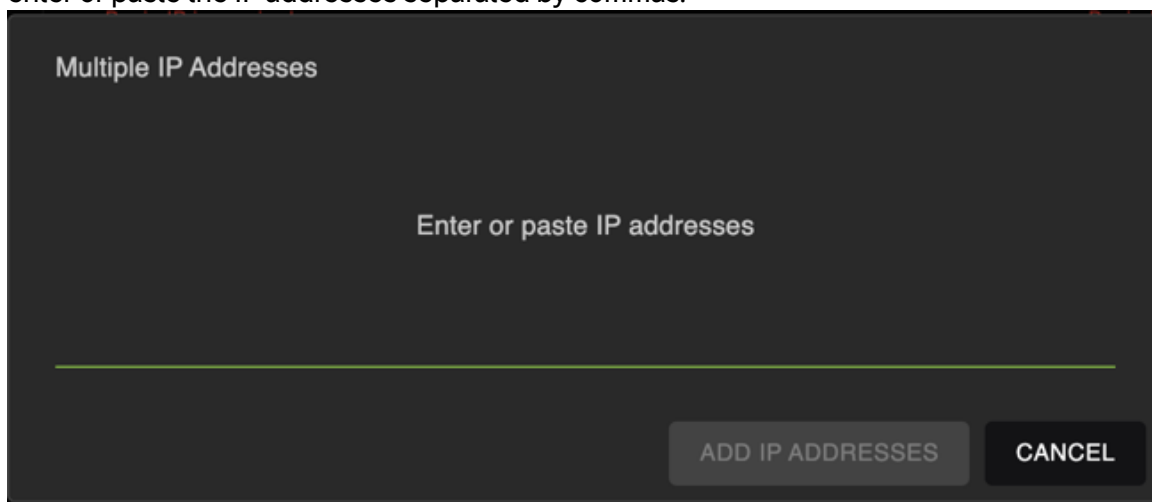
b. Select the **End IP** field and select or enter the ending IP address.

Note: The Console automatically prevents you from selecting the same IPs for both the Begin IP and End IP in both the Include and Ignore sections.

13. Add individual IP addresses to scan:

a. Under Include, select the **IP Address** field, enter a single IP address, and select the add IP address icon .

b. To add multiple IP Addresses at once, select the add multiple IP Addresses icon , and enter or paste the IP addresses separated by commas.



14. Exclude or ignore IP address ranges to scan:

a. Under Ignore, select the **Begin IP** field, and select or enter the starting IP address.

b. Select the **End IP** field and select or enter the ending IP address.

15. Exclude or ignore individual IP addresses to scan:

a. Under Ignore, select the **IP Address** field, enter a single IP address, and select the Add IP Address icon .

b. To add multiple IP Addresses to ignore, select the Add Multiple IP Addresses icon , and enter or paste the IP addresses separated by commas.

Note: You can't include and ignore the same IP address. If you attempt to do so, the system displays an error.

16. Include network zones:

- Under Include, select the **Network Zone** field.
- Select one of the Network Zones from the drop-down menu.

17. Exclude network zones:

- Under Ignore Network Zones, select the **Ignore Network Zone** field.
- Select one of the Network Zones from the drop-down menu.

Note: The Discovery Console for OT automatically prevents conflicts. When you add a zone to the Include list, it is set to unavailable in the Ignore list, and vice versa. This confirms that each zone is assigned to only one list.

18. Optional: If you want to prevent overlapping IP address ranges, select the **Prevent Range Overlap** toggle.

This option helps avoid configuration errors when multiple ranges are defined.

19. On the Sensors page, select Sensor by checking a box next to their name. You can select Sensors in the Allow and Deny sections; but don't select the same Sensor in both sections.

Note: Sensors are online when the circle next to their name is green. A yellow circle indicates Sensors that are offline.

20. After configuring network ranges and zones, review the summary of information.

21. Review all settings, and then select **Create Shared Site**.

Result

The system creates the site and returns you to the Sites page where your new site appears in the list.

Edit or delete a Site

Edit a site to update its information or delete a site that no longer exists on your Discovery Console for OT.

Before you begin

Role required: admin

Procedure

1. Navigate to the Sites page.

Edit a Site

2. To edit a Site, do the following.

- a. Next to the site in the Edit column, select the edit site icon .
- b. Update and save your changes.

Note: You can't select the same IP Addresses for both the Include and Ignore selections for the Site without triggering an error.

Delete a Site

3. To delete a Site, do the following.

- a. Next to the site in the Delete column, select the delete site icon .
- b. Confirm that you want to permanently delete this site, and select **Delete Site**.

Note: If devices are associated to a Site, the Site can't be deleted.

Create a Site-specific Variable set

Create a Site-specific Variable for use in Auto Queries. You can use the **Variable** as a credential for your **Site**.

Before you begin

Role required: admin

About this task

Note: A Site can be associated to only one Variable.

Procedure

1. Navigate to the Variable page in the Console.
2. Create a Variable as described in [Create a Variable set](#).
3. Select a Site to associate with the Variable.
4. Create an Auto Query as described in [Create an Auto Query](#).
5. In the Filter section of the query, select the Sites filter.
6. From the list of sites, select the site associated to your variable.
7. Complete creating the query.
8. Run the Auto Query that you created.

Result

Your Site is associated with the Variable and then queried.

Import Sites

Import existing Sites to the Discovery Console for OT.

Before you begin

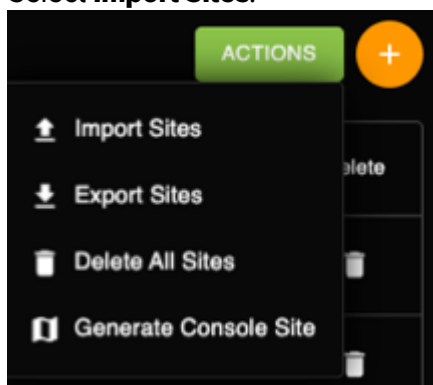
Role required: admin

Procedure

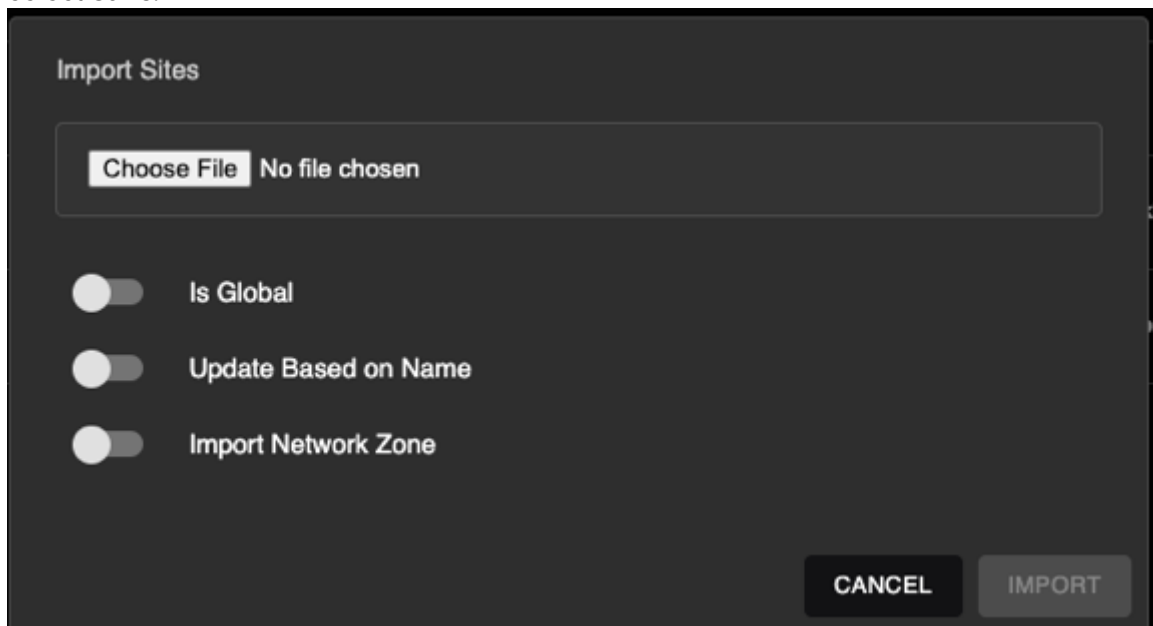
1. Navigate to the Sites page.

Import Sites

2. Select the **Actions** button.
3. Select **Import Sites**.



4. In the Import Sites window, choose the type of site and the file that you want to import, and select **Save**.



Export Sites

5. Select the **Actions** button.
6. Select **Export Sites**.

Result

For the exported site, the Sites information is downloaded in the CSV format.

Note: The CVS file includes an Ignored IPs column when applicable to the Site.

P	Q
NetworkZoneName	IgnoreNetworkZoneName
Nz1	
Nz1	Test NZ1
Nz1	

Export sites

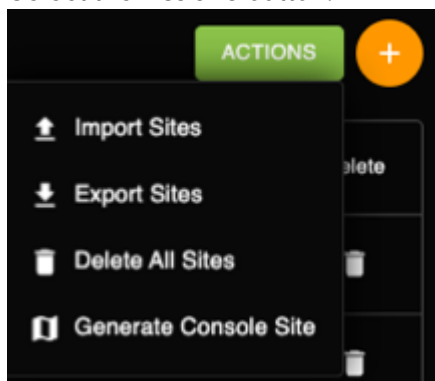
Export Sites on your Discovery Console for OT into a CSV.

Before you begin

Role required: admin

Procedure

1. Navigate to the Sites page.
2. Select the **Actions** button.



3. Select **Export Sites**.

Result

The Sites information is downloaded in the CSV format.

Note: The CVS file includes an Ignored IPs column when applicable to the Site.

P	Q
NetworkZoneName	IgnoreNetworkZoneName
Nz1	
Nz1	Test NZ1
Nz1	

Updates page

The Updates page shows available updates for your Sensor firmware.

The Updates page is organized into the following sections.

Deployment

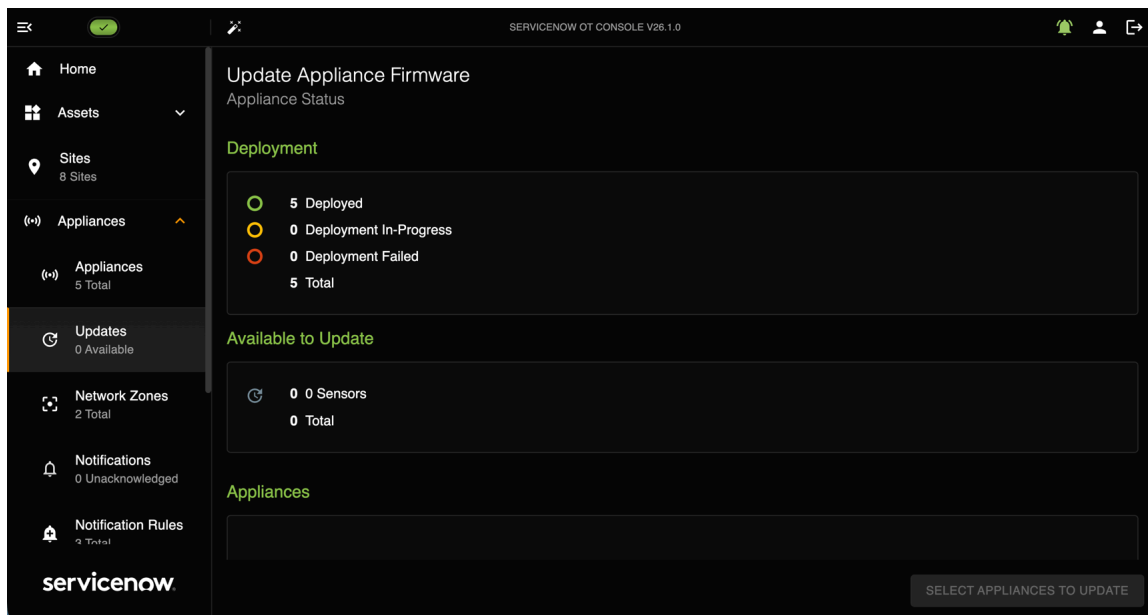
The total number of appliances that are deployed, have deployment-in-progress, or have failed to deploy.

Available to Update

The number of appliances available to update.

Appliances

The appliances that you can select to update. To update the appliance firmware, select the **Select Appliances to Update** button.



Network Zones page

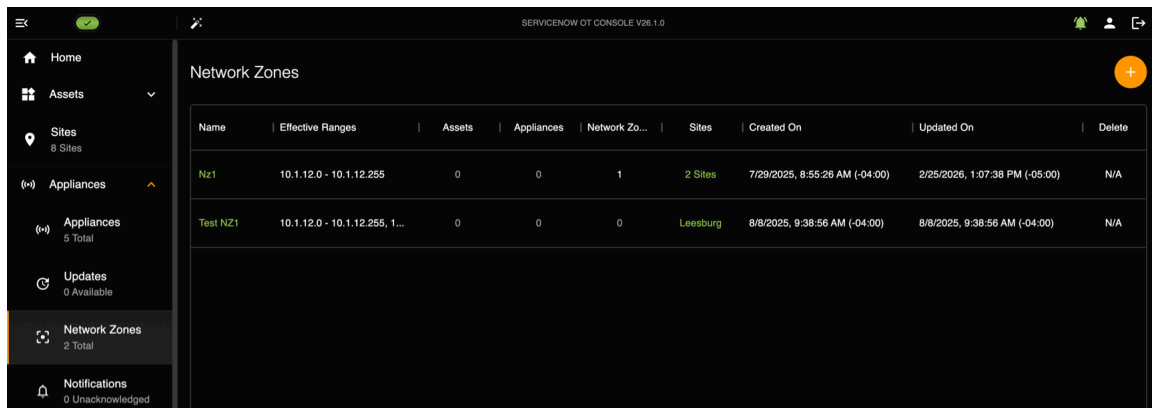
The Network Zones page in the Appliances section includes a list of all Network Zones on the Console. Network zones group assets by IP address to help distinguish one or more assets that share an IP address but are in different local area networks.

Network Zones group assets by IP address to enable the Console to distinguish one or more assets that share an IP address but are in different local area networks (LANs). For example, due to network address translation (NAT). The Network Zones page includes a list of all Network Zones on the Console along with the following details:

- Effective Ranges for Network Zones operations
- Assets related to the Network Zones
- Appliances related to the Network Zones
- Number of Network Zones
- Created On dates
- Updated On dates

Additionally, each of the Network Zones can be deleted when they are no longer in use. You can select the name of the Network Zones to view them in more detail.

The following image shows an example of the Network Zones page.



Name	Effective Ranges	Assets	Appliances	Network Zo...	Sites	Created On	Updated On	Delete
Nz1	10.1.12.0 - 10.1.12.255	0	0	1	2 Sites	7/29/2025, 8:55:26 AM (-04:00)	2/25/2026, 1:07:38 PM (-05:00)	N/A
Test NZ1	10.1.12.0 - 10.1.12.255, 1...	0	0	0	Leesburg	8/8/2025, 9:38:56 AM (-04:00)	8/8/2025, 9:38:56 AM (-04:00)	N/A

Notifications page

The Notifications page shows the notifications available for your Discovery Sensor for Operational Technology (OT).

About this task

You can add a filter to sort and find Notifications related to the following categories.

- End Date
- Rule
- Rule Type
- Severity
- Status

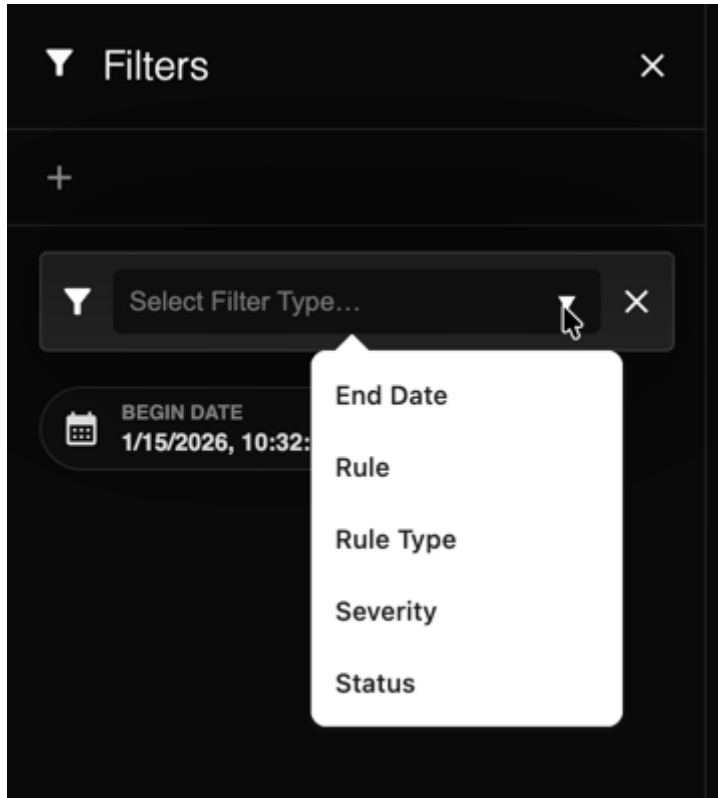
Before you begin

Role required: admin

Procedure

1. Navigate to the Notifications page.
2. To filter the notifications, do the following.

- a. Select the plus icon .
The **Select Filter Type** field opens.
- b. Select a filter from the drop-down menu.

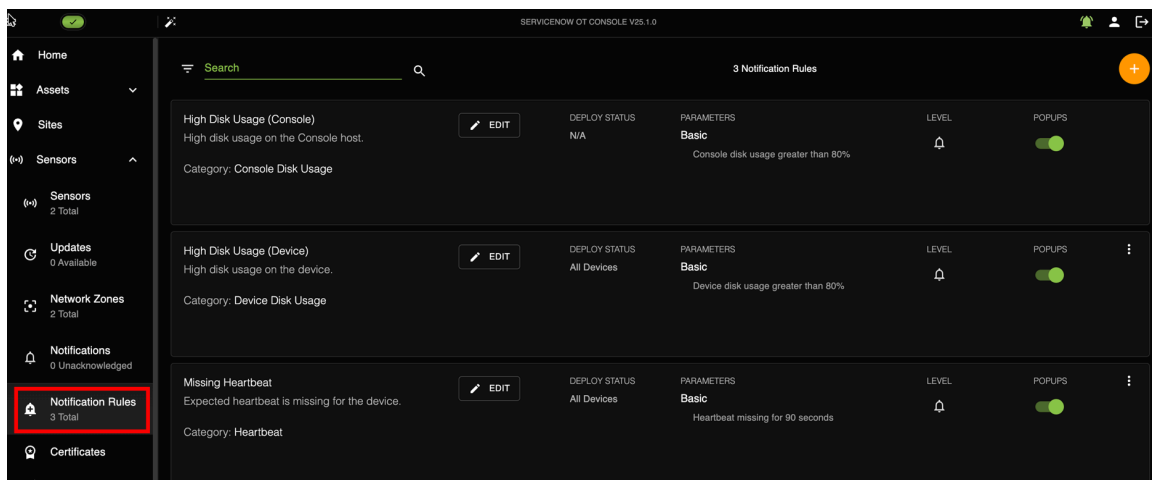


Result

The Notifications are automatically sorted by the selected filter and displayed on the page.

Notification Rules page

The Notification Rules page shows the notification rules that were setup for the Console. Notifications are displayed on the Notification page.



For more information, see [Add a Notification rule.](#)

Add a Notification rule

Create a Notification Rule.

Before you begin

Role required: admin

Procedure

1. Navigate to the Notification Rules page in your Console.
2. Select the add icon .
3. On the form, fill in the following fields.

Notification Rules form

Field	Description
Identification	Name and description for the Notification rule.
Type	Rule type. You can choose from Console Disk Usage, Device Disk Usage, and Heartbeat.
Parameters	Parameters to edit the utilization threshold as needed.
Actions	Add an action for the notification rule from the available list. You can display a message, email, or phone contact. You can also send an email, SMS email, or Syslog. You can add multiple actions to your notification rule.
Notifications	Settings to edit the severity, pop-ups, and suppression of time.

a. Confirmation

Confirm your selections in the previous sections.

4. Select **Create Rule.****Result**

The created notification rule displays on the Notifications page.

Certificates page

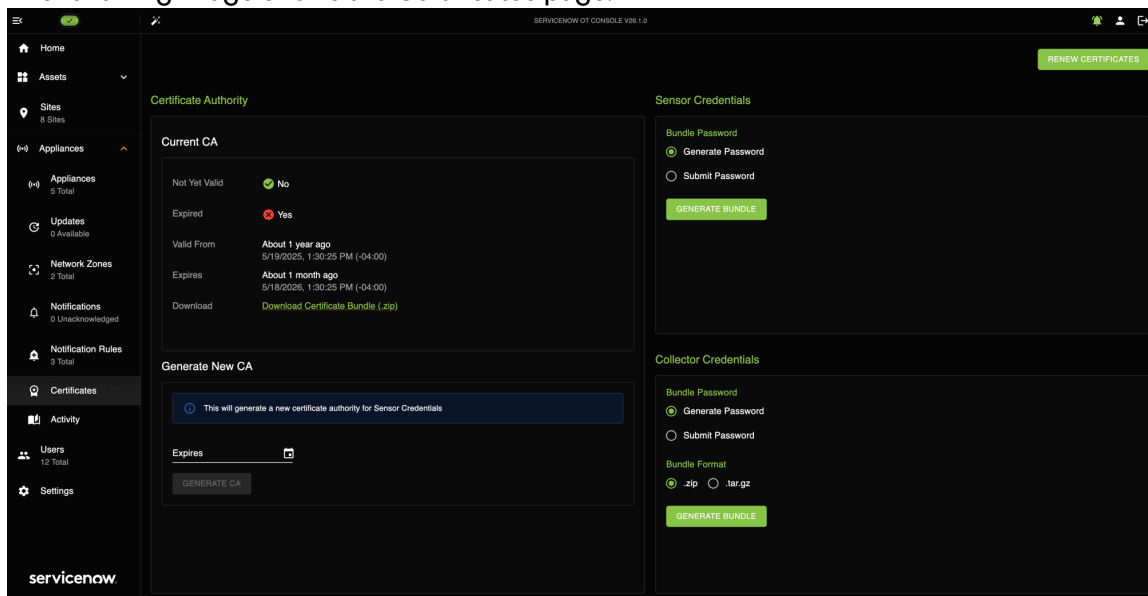
The Certificates page lets you access data regarding your CA certificates, Sensor credentials, and Collector credentials. You can also renew your certifications from this page.

On the Certificate page, you can do the following.

- Generate a Certificate Authority.
- Renew a Certificate.
- Download the Certificate Bundle (.zip).
- Generate a Sensor Bundle using a generated or user-submitted password.
- Generate a Collector Bundle using a generated or user-submitted password. This bundle is generated using the specified bundle format.

Note: For how to renew a certificate, see [Renew a certificate](#).

The following image shows the Certificates page.



Certificate Authority

In the Certificate Authority section, you can generate a new certificate by choosing the expiration date and selecting **Generate CA**.

Select the **Download Certificate Bundle (.zip)** link to download the file containing the Console's Certificate Authority and the server certificate. The certificates establish trust between these applications and confirms their communications are secure and encrypted.

Sensor Credentials

In the Sensor Credentials section, you can generate or submit a password for sensor credentials and then select **Generate Bundle**. The Sensor credentials are formatted in JSON.

Note: The Sensor certificate automatically renews when the Console certificate is renewed.

Collector Credentials

In the Collector Credentials section, you can generate Collector credentials, generate a password bundle, and submit a bundle with either a ZIP file or a tar.gz (tgz) formatted file. Select the ZIP format for Window collectors and the tar.gz format for Linux collectors.

Note: The Collector credentials are formatted in JSON.

When ready, select **Generate Bundle**.

Note: The certificate for the Discovery Console for OT and the Discovery Sensor for OT automatically renews when it is within 30 days of its expiration date.

Renew a certificate

This section describes how to renew a certificate on the Certificates page.

Before you begin

Role required: admin

Procedure

1. From the Certificates page, select the Renew Certificates button.

2. The prompt window opens.

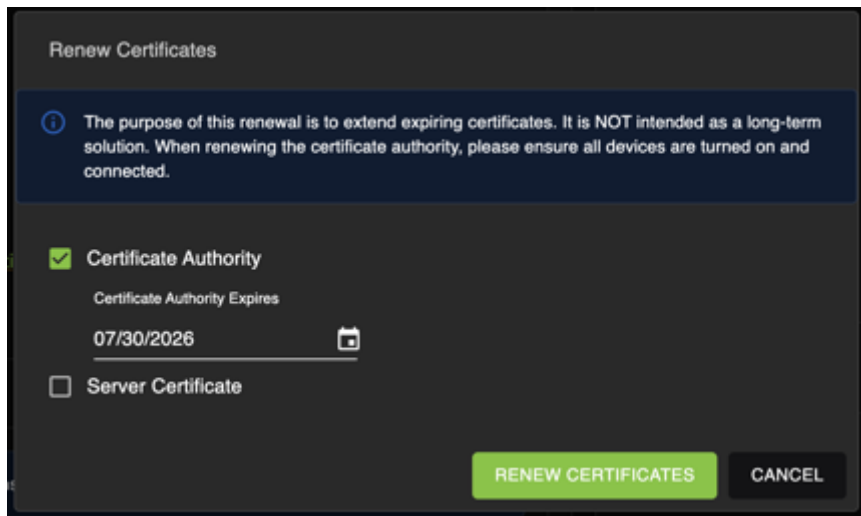
The prompt reads: The purpose of this renewal is to extend expiring certificates. It is NOT intended as a long-term solution. When renewing the certificate authority, verify all devices are turned on and connected.

3. Check the box next to either the Certificate Authority or the Server Certificate.
For this example, the Certificate Authority is chosen.

4. The **Certificate Authority Expires** appears with a pop-up calendar at the end of the line.

5. The calendar opens for you to choose an expiration date.

6. Once you have chosen a date, it appears in the window after the Certificate Authority.



- Note:** This renewal does not generate a new private key pair. The Console keeps track of old and the new certificates. To avoid issues, renew the Sensors and Collectors certificates at the same time. Renew all certificates at least 48 hours before the expiration date and verify that all devices are online to verify the automated retrieval occurs. After they are retrieved, there is a small interruption as the Sensor and Collectors restart to load the new certificates.

Activity page

The Activity page lists only the Appliance activity on your system.

Your Appliance activity is organized by the most recent activity and shows the date and time the activity took place. The page also displays the Appliance name, the type and subtype of activity, and any additional details.

Users page

The Users page shows the lists of both active and inactive users in your Discovery Console for OT system. You can access the Discovery Console for OT through user accounts available in the system.

User overview

The following user accounts are available in the system.

- Administrator accounts, which have full access to the Discovery Console for OT's functionality and features
- Non-administrator accounts, which have limited access to the Discovery Console for OT

- Note:** Each user who needs access to the console is given a user account with private credentials. The Console application records user activity in the system. Sharing accounts or account passwords prevents an accurate audit of system activity.

Registering the initial user

When the Discovery Console for OT is accessed for the first time after installation, the console guides the operator through the initial user registration process. The initial user account is created as an administrator account and has access to all features of the application.

The following sections describe how to create and register the initial user.

Step 1: Accepting the End User License Agreement

You must read and accept the End-User License Agreement (EULA) before you can set up the initial user. Confirm that an individual with legal authority and authorization has also reviewed the EULA before accepting the agreement.

Step 2: Creating the Initial User

After you accept the EULA, you're prompted to register the initial user. A username, password, and email address are required to complete the account setup. You must complete all of the fields before you can register the user.

The initial user is automatically assigned the administrator role and has full access to the system. Save the password for the initial user account in a secure place. The administrator account is necessary to create accounts for additional users.

Note: If all administrator accounts are inaccessible, contact your Discovery Console for OT representative for assistance.

Managing user accounts

On the Users page, you can view all of the users in the system. Administrators are the only users that can list, create, or view information and update another user's information in the system. Administrators can also force a user to change their password on their next log in.

To view a user's information, you can select the user on the Users page.

User roles

When creating user accounts, you can assign the following roles.

Note: You can assign more than one role to a user.

Discovery Console for OT roles

Role	Description
Admin	Can access the full functionality of the Discovery Console for OT. Can create, edit, and remove user accounts.
Reader	Can view the Discovery Console for OT with read-only permissions.
User	Can access the Discovery Console for OT with limited permissions.

Note: For more information, see [Set up a Microsoft Entra ID](#) next.

Set up a Microsoft Entra ID

This section describes how a Discovery Console for OT user can set up an **Microsoft Entra ID** integration.

Before you begin

Role required: admin

About this task

The **Microsoft Entra ID** integration enables users to log in to the Discovery Console for OT using their organization's **Microsoft Entra ID** cloud identity access management (IAM) credentials.

This removes the need for managing separate usernames and passwords within the application.

This feature relies on configuring an application in **Microsoft Entra ID** and providing the required details in the Console settings.

Note: This feature requires the Discovery Console for OT to have internet access.

This integration allows seamless and secure authentication using **Microsoft Entra ID**, improving user experience and aligning with enterprise identity management practices.

To enable an **Entra ID** log in, an administrator must complete the following steps.

Note: Check with Microsoft for the latest documentation before you begin this procedure.

Procedure

1. Register an application in Entra ID.

2. In the Azure application:

- a. Navigate to **Entra ID > App** registrations.
- b. Create a new application; for example "Console app".
- c. Configure a Redirect URI pointing to the Console URL; for example, <https://<console-url>>.

3. Collect required values.

From the Entra ID application, locate the following information.

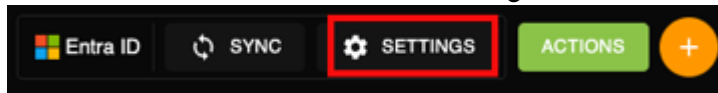
- Domain: Organization's primary domain, for example, company.onmicrosoft.com.
- Tenant ID: Found in the Entra ID **Overview**.
- Client ID: Application (client) ID from App registration.
- Client Secret: Generated under **Certificates & secrets**.
- Object ID: Application object ID.

4. Configure Console settings.

5. In the Discovery Console for OT:

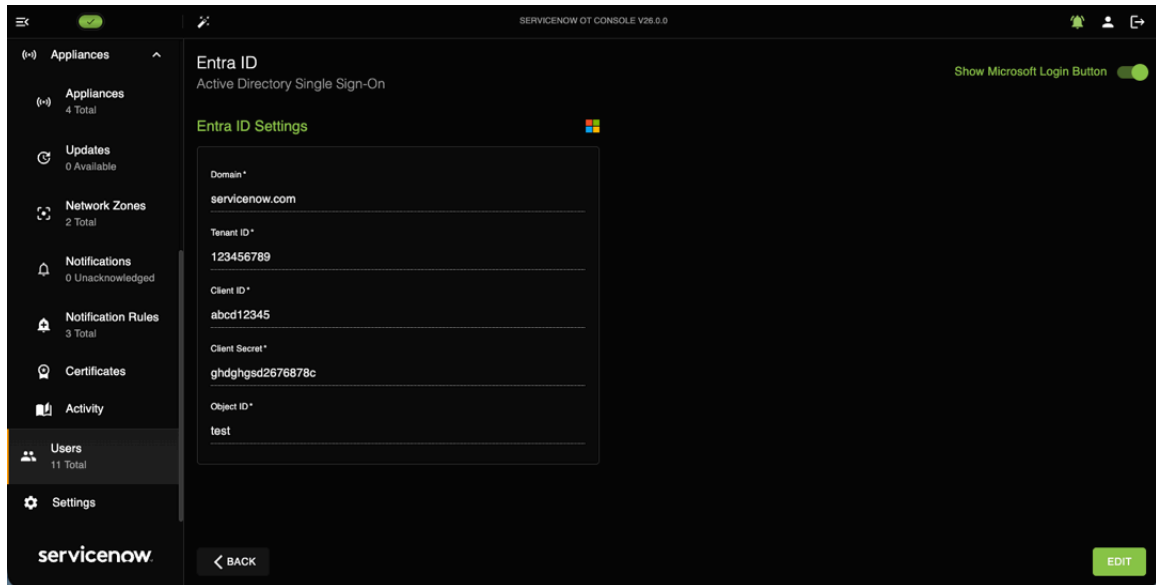
a. Navigate to **Console > Users**.

b. Next to the **Actions** button, select **Settings**.



c. Enter all required values.

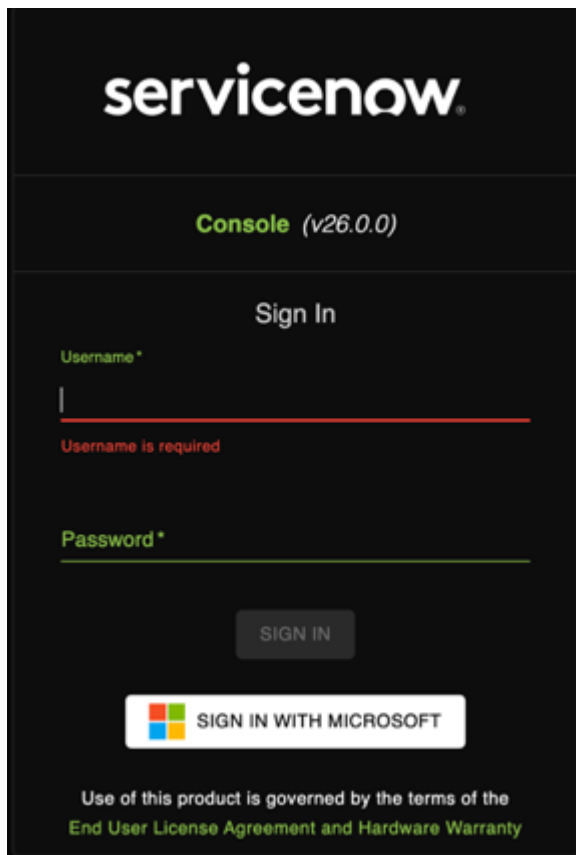
- Domain
- Tenant ID
- Client ID
- Client Secret
- Object ID



d. Select **Save**.

6. Enable the log in option.

- In the Entra settings, toggle **Show Microsoft Log in button**.
- This enables the SSO log in for end users.



Result

Once configured, user can log in by doing:

1. Open the Console log in page.
2. Select the **Sign in with Microsoft** button.
3. Authenticate using the organization's Microsoft account.
4. After successfully authenticating, the user is redirected to the Console and is logged in.

Note: Important considerations:

- The Client secret must be kept secure and renewed before expiration.
- The redirect URI in Entra must exactly match the Console URL.
- Incorrect Tenant ID or Client ID results in authentication failures.
- Admin consent may be required when configuring permissions in Entra.

Create a user

Create a user account that can access the Discovery Console for OT.

Before you begin

Role required: user

Procedure

1. Navigate to the Users page.
2. Select the add icon .
3. On the form, fill in the following fields.

Add user form

Field	Description
Username	Username for the user account.
Email	Email for the user's account.
Password	Secure password for the user account.
Confirm Password	Retype the password.
Roles	Roles that the user account needs. If needed, you can select more than one role.

Edit a user's information

Edit a User's information and keep the user account up to date.

Before you begin

Role required: admin

Procedure

1. Navigate to the Users page.
2. Select the user account that you want to modify.
3. Select **Edit**.
4. Edit the available fields as needed.
5. Select **Save**.

Force a password reset

Force a user to reset their password.

Before you begin

Role required: admin

About this task

An administrator can force another user to change their password the next time that user logs on to the Console.

Procedure

1. In the Console, navigate to the Users page.

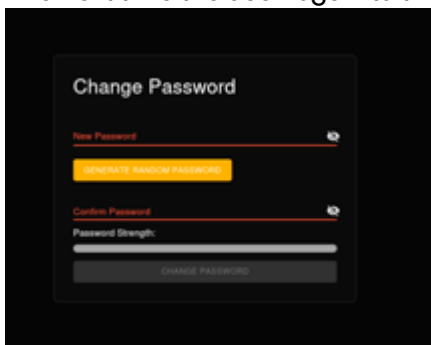
2. You can force a user to change their password by clicking on the green key.

3. Refresh the page.

The green key changes color to an orange key with backwards slash through it. This means the user needs to change their password the next time they log in. The key image does not display once the user changes their password and logs back in.



The next time the user logs into the console, the **Change Password** window opens.



4. Enter a new password and then enter it again to confirm it.

For guidance, the Change Password window displays the Password Strength.

5. Select **Change Password**.

Deactivate a user

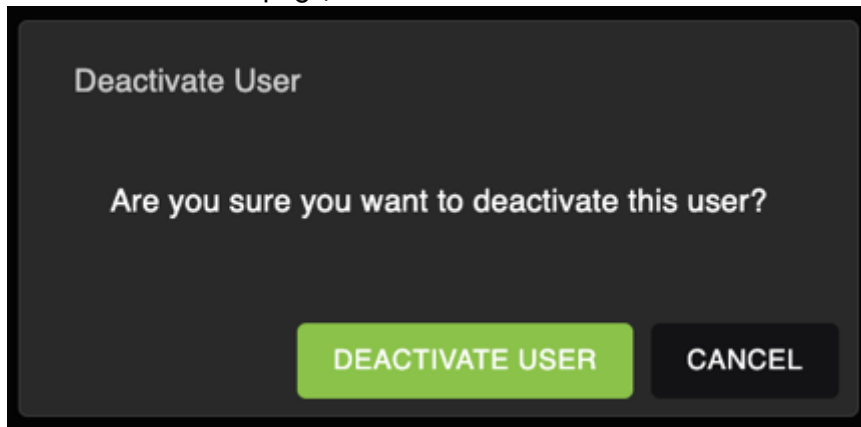
Deactivating a user verifies that they can't access the Discovery Console for OT.

Before you begin

Role required: admin

Procedure

1. Navigate to the Users page.
2. Next to the user you want to deactivate, select the Deactivate User icon .
3. On the confirmation page, select **Deactivate User**.



Settings page

The **Settings** page lets you view and modify system-wide settings for the Discovery Console for OT, Discovery Sensor for OT, and the OT Discovery Collector.

Settings page overview

To open the Settings page, select **Settings** from the main navigation menu. The Settings page is divided into tabs and opens to the **Console** tab view. The Settings page is organized by the following tab configuration options.

Console

The Console tab on the main Settings page is divided into the following sections.

- **About**

The Console tab includes a link to the End-User License Agreement (EULA), the version number of the Console, and the Console ID.

- **License**

When you first sign into the Console, a warning banner alerts that you need a license. When you use the interactive configuration wizard, you're also alerted to the license status. For more information, see [Requirements for Discovery Console for OT installation](#).

Note: If needed, request a Console license from your ServiceNow account representative.

- **Configuration**

The Configuration section displays the Console Name of the local web Console. The Console Name is used in Syslog messages.

In the Configuration section, use the **High Contrast** setting to change hyperlinks from orange to green for ease in viewing. To change this setting, select the **Edit** button, then slide the **High Contrast** toggle to **Yes**. Select **Save** to save your changes.

Configuration

Console ID 4ea9ea4f-5a05-484c-bf0d-3665338d1c25	Console Name Console
DNS Server (IPv4)	Latitude (degrees, -90 to 90)
Longitude (degrees, -180.0 to 180.0)	Autoload Asset Graph No
High Contrast Yes	

System Statistics

EDIT

• System Statistics

The Console settings show disk and memory usage for its host server. It's important to maintain an adequate disk and memory space so that the Console continues operating properly. Check the system statistics periodically to confirm that proper resources are available.

Certificate

On the Certificate tab, you can check the Console Certificate status. You can also update the certificate by selecting Generate New Bundle or Upload Bundle (.p12) and then selecting the **Generate Bundle** button.

Note: The Certificate tab does not function the same as the **Certificates** page.

API

The API settings manage active and denied tokens and provide endpoint configuration files for the Service Graph Connector for ServiceNow OT Discovery.

Email

The Discovery Console for OT can be configured to send email and SMS text alerts when certain conditions occur within the system. To do so, the Console relies on an external mail server to send messages.

In the Email Server Configuration panel, enter the settings that match your mail server configuration. The Discovery Console for OT uses these settings whenever the **Enable Alert Notifications** setting is activated.

Exports

The Export tab downloads data from the Console to JSON files. Available data types include Assets, Sites, Software, Sensors, Network Zones, Notifications, Images, and All. Selecting All bundles and downloads data from all categories in one ZIP file.

Metadata

The Metadata tab includes settings for several features related to metadata that can be used to enrich the analysis and reporting of data collected by the Console. For example, you can set up metadata to provide more details about the connections observed in the network.

The following table describes the different sections of the Metadata tab.

Section	Description
CVE Database Package	Enables you to import a CVE package. You can use the Import CVE Package button to import a package locally saved on your computer. Note: You can obtain a current CVE database file from your ServiceNowOperational Technology Discovery representative.
Query Driver	Enables you to import or download query drivers and set the concurrence and speed of Sensor and Scout queries. You can use the Import Query Driver button to import a query driver from your computer or Download Query Driver to download the current query driver and save locally. To edit the Query Driver settings, select the Edit Settings button.
Common Port Names	Defines a mapping between port numbers and protocol names. This information is used in the Console to display protocol names when you create a ports activity report. This feature must be turned off to import a new port name file. To enable or disable this setting, select the Edit button under the Common Port Names and Ethernet vendor sections. A current port names file can be obtained from your Discovery Console for OT representative.
Ethernet vendors	Defines a mapping between MAC addresses and vendor information. This information is used in the Console to provide vendor information for assets. This feature must be turned off to import a new Ethernet vendors file. To enable or disable this setting, select the Edit button under the Common Port Names and Ethernet vendor sections. A current Ethernet vendors file can be obtained from your Discovery Console for OT representative.

Package

In the Package tab, you can use the package source options under the **Package Manager Configuration** section. You can import packages by file upload or from a remote repository.

Note: The package manager must be configured so that your Discovery Console for OT sensors can receive firmware updates.

Reprocess

The Reprocess feature allows the system to reevaluate previously collected Auto Query scan results using the latest query driver logic. See [Reprocess Auto Query results](#) for more information.

Syslog

In the Syslog tab, you can configure a Syslog server. After configuring these settings, Syslog data can be forwarded from the Discovery Console for OT to a separate Syslog data consumer. For example, the Splunk enterprise security data analysis tool set.

Logs

From the Logs tab, you can download Discovery Console for OT logs. You have the option to choose whether to download logs on the current day, on a custom date, or on a date range.

For more information, see [Download Console log files](#).

Certificate tab

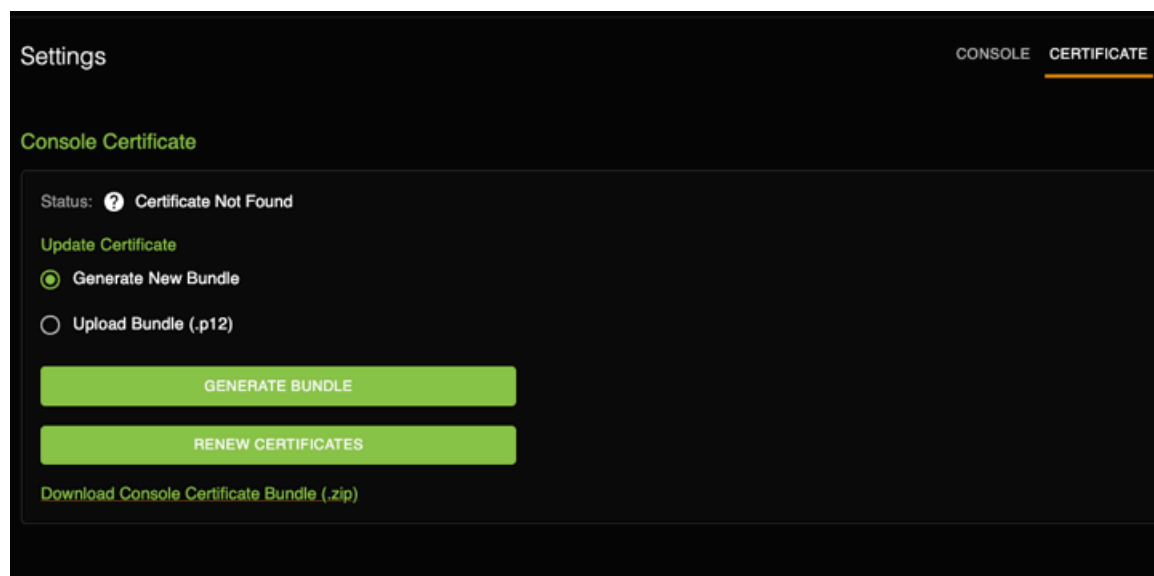
The Certificate tab is for generating or uploading the Discovery Console for OT certificate.

Console Certificate

The Console generates its own self-signed certificate bundle when initially deployed. The Certificate tab is for updating, generating, uploading, or downloading a Console Certificate.

On the Certificate tab you can select from the following actions to update a Console Certificate:

- Generate New Bundle.
- Upload Bundle (p12).
- Download the Certificate Bundle (.zip).
- Renew Certificates.



After you generate a New Bundle, you can select the link **Download Console Certificate Bundle (.zip)**. The bundle contains the Console's Collector Certificate Authority and the RabbitMQ certificate. These certificates establish trust between the Console and Collector and confirms their communications are secure and encrypted.

- Note:** For more information, see [Renew a certificate](#). The steps are similar but the Certificate tab only pertains to the Console Certificate.

Discovery Console for OT API

You can access the discovery data from the Console via the API. On the Settings page, select the **API** tab to view and use the active tokens, denied tokens, and endpoints needed to communicate with the Service Graph Connector (SGC).

- Note:** For more information, see [Service Graph Connector for ServiceNow Operational Technology \(OT\) Discovery](#).

API settings

The API settings are used to set up the active tokens, denied tokens, and endpoints needed to communications between the Service Graph Connector for ServiceNow OT Discovery and the Operational Technology Discovery components.

Tokens can be imported or exported, and endpoints can be downloaded.

The Service Graph Connector for ServiceNow OT Discovery enables the API to communicate data from the Discovery Console for OT and other Discovery components to the ServiceNow instance. Data can also be communicated to and from external APIs.

Functionality

The Service Graph Connector for ServiceNow OT Discovery has been enhanced for better connection to and from the Discovery components, the Discovery Console for OT API, and your ServiceNow instance.

The Service Graph Connector for ServiceNow OT Discovery makes available for the Discovery Console for OT API functions such as:

- Sends the status of the user license.
- Imports all software programs that are identified on the devices and returns a paginated list from the SoftwaresAPI view.

The API ingests software and provides the following program attributes:

- `inputProduct`: Software name
- `Version`: Version of the installed software
- `inputVendor`: Manufacturer of the software
- `lastSeenOn`: Assets' LastSeenOn field added to the object
- `assetId`: Derived from the `_id` for the asset document containing the software array.
- `_id`: For the document; should be the `_id` for the object in the software array
- Transfers images and screen shots from the Console to the ServiceNow instance. This returns images in a paginated list with these filters:
 - `UpdateOn`
 - `CreatedOn`
 - `ScreenShot`
 - `Size`
 - `OCR Words`
 - `Titles`

- Pushes Discovery Sensor for OT information to the ServiceNow instance.
 - The API can be used to return the `sensorId`.
 - You can gather information about the Sensor and use it to discover assets.
 - Sensor information can be pushed via the API to the ServiceNow instance.
- Sends to the Console virtual machine (VM) health metrics and host metrics of the Sensor and the Collector. This helps with visibility of version, installed processes, and the health of the host machine for the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector.

Indirect network connection (air-gapped)

For security reasons, a computer or system may not be directly connected to the internet or may be on an unsecured LAN. In such a situation, the Operational Technology Discovery components can't push files or data to the MID Server and from there via the Service Graph Connector on to the ServiceNow instance.

To solve the air-gap issue, the Discovery Console for OT can generate JSON files. These JSON files are physical files and can be manually copied and then moved to the MID Server via an external drive. They can then be manually copied to a specific directory on the MID Server and then consumed through the SGC to the ServiceNow instance.

For example, if you navigate to **Settings > Exports** on the Discovery Console for OT, you can download data generated by the Discovery components as a JSON export file. You can schedule the frequency of these downloads setting the number of days and time of day. These files are saved to the `/opt/MSi/srv/apieexports` directory. From there you can move them to physical media like a thumb drive. You can then copy or import the JSON files to the MID Server and through Service Graph Connector for ServiceNow OT Discovery and then on to the ServiceNow instance.

Related topics

[Air-gapped networks and OT Discovery installation](#)

[Export data](#)

[Edit API settings](#)

[Create a backup for the Console](#)

Edit API settings

Edit the API settings for the Discovery Console for OT to generate active tokens, remove denied tokens, or view the available API endpoints needed to communicate with the Service Graph Connector for ServiceNow OT Discovery.

Before you begin

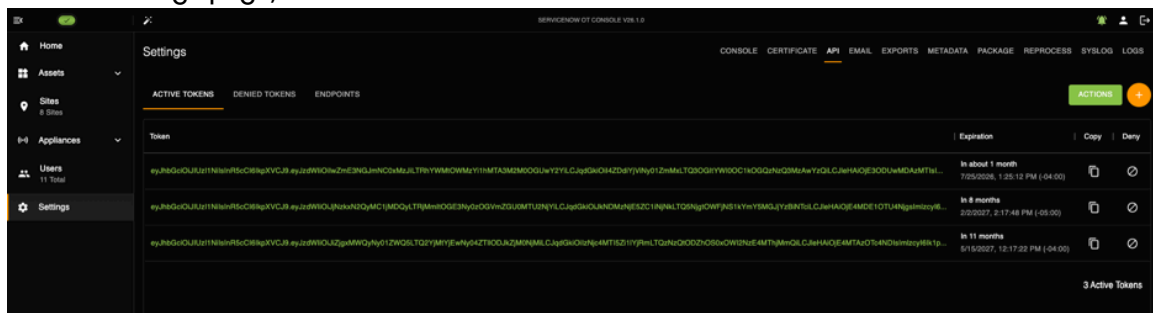
Role required: admin

About this task

The Service Graph Connector for ServiceNow OT Discovery has been enhanced to make available these functions of the Discovery Console for OT API.

Procedure

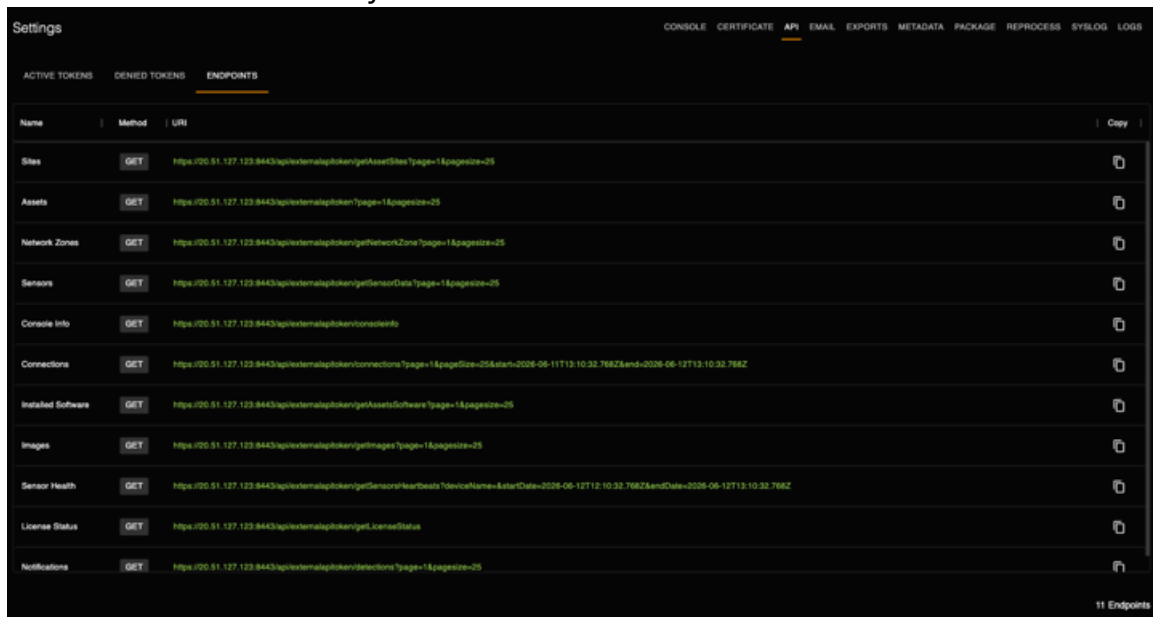
1. In the main menu, go to the Settings page.
2. On the Settings page, select the **API** tab.



Active Tokens

3. Generate an API token.
 - a. Select the **Active Tokens** tab.
 - b. Select the add icon .
 - c. In the Generate API Token window, select the expiration date.
 - d. Select **Generate Token**.
4. Remove denied tokens.
 - a. Select the **Denied Tokens** tab.
 - b. Next to the API token that you want to remove, select the **Remove Token**  icon.
5. View the available endpoints.

The endpoints are listed in columns by name, method, and their URI. The following endpoints are available for the Discovery Console for OT.



- **Sites**
- **Assets:** Returns the DeviceId for each asset; if no DeviceId is set, then it returns null.
- **Network Zones:** Returns values for the Network zone, parent/child zones, Subnet information, and IP ranges.

- **Sensors:** Returns the Sensor id (`sensorId`) that points to the sensor that was used for the discovery.
- **Console Info:** Returns the Console information.
- **Connections**
- **Connections-V2**
- **Installed Software**
- **Images**
- **Sensor Health**
- **License Status:** Returns the status of the license and whether it is expired, to the Discovery Console for OT.
- **Notifications**

a. Select the **Endpoints** tab.

b. Select the copy icon () to copy the endpoint.

c. The data is matched to the API.

d. Automatically store files under `./apiexports`.

e. Use the naming convention `${API}_${DATE}.json` (for example, `Assets_19791231.json`).

f. After creating the new file, delete any previously created files.

g. Only generate files if there is sufficient disk space.
The disk space available is limited to 1 GiB.

Edit email settings

Edit the email settings as needed to match the settings on your mail server.

Before you begin

Role required: admin

Procedure

1. Navigate to the Settings page.
2. Select the **Email** tab.
3. Select **Edit**.
4. On the Email Server Configuration form, edit the following fields as needed.

Email Server Configuration

Field	Description
Host	IP address of the email server.
Port	Port of the email server. Typically port 25.
From Address	From address to use for the alert

Field	Description
Enable TLS Encryption	Setting that must match the TLS setting on the email server.
Enable Connection Logging	Option to log all email server connections to a file

5. Select **Save**.

Export data

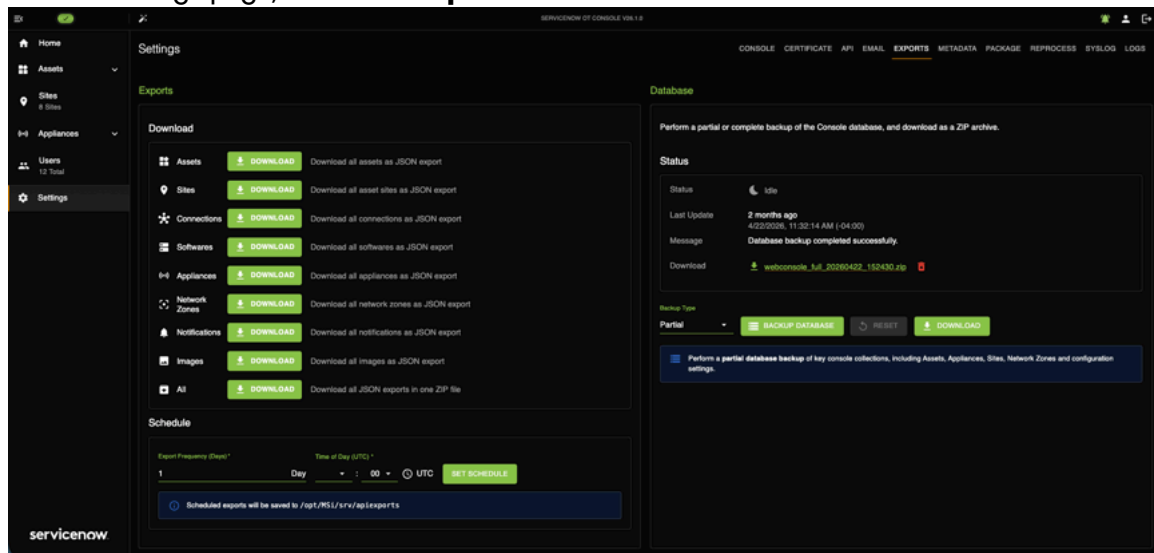
The Discovery Console for OT exports data as a JSON export file.

Before you begin

Role required: admin

Procedure

1. In the main menu, select the **Settings** option.
2. On the Settings page, select the **Exports** tab.



Note: For information, see .

3. Select and export data into JSON files.
The available data includes the following.

- Assets
- Sites
- Connections¹
- Softwares
- Sensors
- Network Zones
- Notifications
- Images
- All

1. There are two version of Connections API. They provide the same information in two different formats.

© 2026 ServiceNow, Inc. All rights reserved.

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 names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Selecting **All** downloads all JSON exports to one zip file.

4. Select the **Download** button next to the desired data.
The scheduled exports are saved to /apiexports.
5. Under the **Schedule** heading, select the export frequency by number of days and time of day (UTC).
The default frequency is 1 day. The time-of-day defaults to 00:00 AM UTC.

Create a backup for the Console

You can create a full or partial backup of the Discovery Console for OT data.

Before you begin

Role required: admin

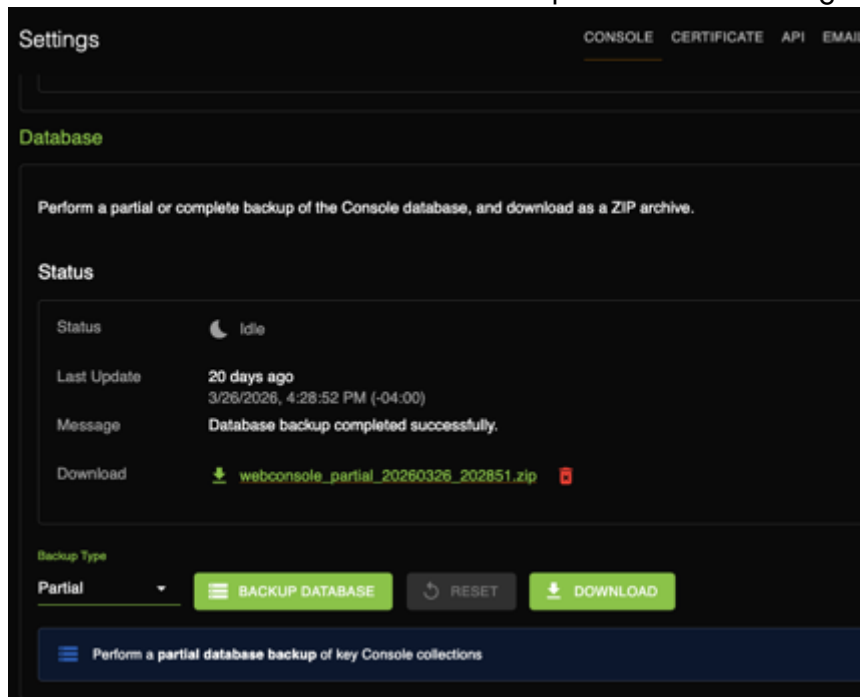
About this task

To create a backup for the Console, you must have **admin** access.

To support disaster recovery, the Discovery Console for OT generates backup files containing restore data, configuration, and logs. Console administrators can initiate backups and restore the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector to their previous states when needed. This enhancement provides reliable disaster recovery capabilities across all system components.

Procedure

1. Navigate to **Settings > Export** tab.
2. Use the **Database** section to create a backup of the Console MongoDB.



3. Select the **Backup Type** and select from the drop-down menu.

- A **Full** back up includes:
 - entire WebConsole database
 - all images
- A **Partial** backup only includes the collections defined in the `PartialIncludeCollections` setting in `appsettings.json`.

4. If you select a **Partial**, the downloaded ZIP file, by default, includes only the following collections.

- AssetAutoScans
- AssetDeviceMessages
- AssetDeviceStatistics
- AssetDevices
- AssetProperties
- AssetRevisions
- AssetScanResults
- AssetScanResultsArchive
- AssetScans
- AssetSites
- Assets
- CyberDashboards
- DetectionRules
- DetectionScoreDetails
- Detections
- DeviceErrors
- DevicePolicyStatus
- DeviceScoreDetails
- DeviceWhitelistApplicationPermissions
- Devices
- EthernetVendorOrganizations
- EthernetVendorRanges
- EthernetVendors
- ExternalAssets
- NetworkZones
- Settings
- UnsafePorts

Image files aren't included in a Partial backup.

5. Archive data can be included or excluded based on the system configuration.

6. You can set system configurations during the Console installation process.

7. The backup behavior for archived query results is controlled by the following Backup configuration settings in the `appsettings.json` file.

- If `ExcludeArchiveFromFull` is set to **true**, archived scan results are excluded from the Full backup.
- If `ExcludeArchiveFromFull` is set to **false**, archived scan results are included in the Full backup.
- If `ExcludeArchiveFromPartial` is set to **true**, archived scan results are excluded from the Partial backup.
- If `ExcludeArchiveFromPartial` is set to **false**, archived scan results are included in the Partial backup, provided that `AssetScanResultsArchive` is listed in `PartialIncludeCollections`.

a. Full backup

- If `ExcludeArchiveFromFull` = `true` Archive **NOT included**
- If `ExcludeArchiveFromFull` = `false` Archive **INCLUDED**

b. Partial backup

Even though `AssetScanResultsArchive` is in your list for backup in configuration:

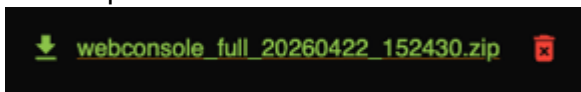
- If `ExcludeArchiveFromPartial` = `true` Archive **NOT included**
- If `ExcludeArchiveFromPartial` = `false` Archive **INCLUDED**

8. After deciding the **Backup Type**, select the **Backup Database** button.



9. When the backup is finished, the screen displays "Database backup completed successfully."

10. A backup ZIP file is available to download.



11. Select the **Download** button and the ZIP is downloaded to your local system.

12. Once the file is downloaded, select the delete icon (trash can) to remove the archive and free up disk space on the Console.

Edit the Query Driver on Metadata tab

Edit the Query Driver on **Metadata** tab. The Query Driver section enables you to import or download query drivers and control the speed of Auto Queries.

Before you begin

Role required: admin

About this task

On the Settings page, the **Metadata** tab includes settings for several features related to metadata that enhance analysis and reporting in the Discovery Console for OT. The **Query Driver** settings control your Sensors' performance and resource usage. These settings manage how quickly Auto Queries are executed and how much load is placed on your network devices. They also regulate how many queries a Sensor can execute simultaneously. The **Delay** setting specifies the interval between consecutive queries. For example, setting the delay to 50% effectively halves the time between queries and operating the query at a faster pace.

Procedure

1. Navigate to the **Settings > Metadata** tab.
2. In the Query Driver section, you can import or download the Query Driver.
3. To edit the Query Driver, select the **Edit Settings** button.
The **Query Driver Settings** window opens.
4. In the Sensor Load section of the window, use the sliding scale to change settings for the Query Load and the Discovery Load.
5. In the Delay section of the window, use the sliding scale to change the Query Delay settings.

The screenshot shows the 'Query Driver Settings' window with a dark theme. At the top right is a close button (X). The 'Sensor Load' section contains an information box with an 'i' icon and the text 'Concurrent queries per sensor'. Below this are two sliders: 'Query Load' with a value of 10 and 'Discovery Load' with a value of 5. Both sliders have a scale from 1 to 25. The 'Delay' section contains a 'Query Delay' slider with a value of 75.5% and a scale from 1% to 100%. At the bottom right are two buttons: 'SAVE SETTINGS' (green) and 'CANCEL' (dark grey).

6. Select the **Save Settings** button to save, or the **Cancel** button to discard your changes.

Upload firmware packages

If you're using a local repository, upload firmware packages to the Discovery Console for OT so the system knows when an update is needed.

Before you begin

Role required: admin

Procedure

1. Obtain the latest firmware packages directly from your Discovery Console for OT account representative.
2. Navigate to the Settings page and open the **Package** tab.
3. Select **Import Packages**.
4. Select the provided firmware package and select **Open** to upload the files.
The Package Import status modal window tracks the upload status.
5. Repeat steps 2–4 for each firmware package.

Result

The Discovery Console for OT verifies the integrity and authenticity of the uploaded file before they're made available for device updates. Packages that fail authenticity checks are automatically rejected during the upload process.

Reprocess Auto Query results

On the Settings page, the Reprocess tab is available to reprocess Auto Query results.

Reprocess feature

The Reprocess feature allows the system to reevaluate previously collected Auto Query scan results using the latest query driver logic. This is useful when a query driver(s) is updated. Instead of rescanning devices, the system reuses existing stored scan results and processes them again. The results display on the Results page.

The Reprocess feature runs based on the configured schedule. As displayed in this table, you can schedule your configuration.

Configurations

Setting	Options
Start time	Default: 12:00 a.m. UTC
Run Mode	• Always • Only when the Query Driver version changes (default setting)
Scope	• Results only • Results + Archived Results
Time range	Last 17 days, Last 30 days, or Custom. Default is the last 14 days.
Duration	Until completed or time-limited
Batch size	No default.
Enable?	Yes / No

After upgrading to a new query driver version, enable the Reprocess schedule to reevaluate recent scan results using improved logic.

Settings

CONSOLE

CERTIFICATE

API

EMAIL

EXPORTS

METADATA

PACKAGE

REPROCESS

SYSLOG

LOGS

Auto Query Results Reprocess

Reprocess is running

Note: Default Start Time is 00:00 UTC (midnight). Scheduled reprocess runs once per UTC day. To run again on the same day, click Run Now.

RUN NOW

STOP REPROCESS

CLEAR STOP

RESET STATE

REFRESH

Schedule & Run Settings

Current State

Enabled?

No

Start Time (UTC)

Hour

Minute

0

00

Run Mode

Only when driver updated

Scope

Results

Time Range

Last 14 days

Duration (hours)

0

0 = until completed

Batch Size

200

Status

RUNNING

Processed

495

Skipped (No AssetId)

148

Skipped (Already processed)

0

Last Checkpoint: 2026-02-12 15:39:08.666 UTC

In Progress

Yes

Stop Requested

No

Paused for Duration

No

Can Resume From Last Checkpoint

Yes

Resume From Archive Results

No

Auto Queries Paused (Count)

1

Current Run Driver Version

5.27.0

Last Processed Driver Version

5.27.0

Last Run Started (UTC)

2026-02-18 15:11:49.340 UTC

Last Run Completed (UTC)

2026-02-12 16:12:18.444 UTC

EDIT

Edit Syslog settings

Edit the Syslog settings as needed to configure the Syslog server.

Before you begin

Role required: admin

Procedure

1. Navigate to the Settings page.
2. Open the **Syslog** tab.
3. Select **Edit**.
4. On the form, edit the following fields as needed.

Email server settings

Field	Description
Host	IP address of the Syslog host
Port	Port that the host listens on. Typically port 514 for Syslog.
Transport	Transport protocol used by the host. Typically, UDP.
Facility	Descriptor used to indicate which process on the machine created for the Syslog event.
Level	Desired Syslog severity level that's pushed to the receiving server.
Audit Log Messages	If toggled on, enable Audit Log Messages.

5. Select **Save**.

Important: Be sure to adjust any network firewall rules to open the specified Syslog port and protocol. Otherwise, traffic from the Discovery Console for OT can't reach the receiver application.

Download Console log files

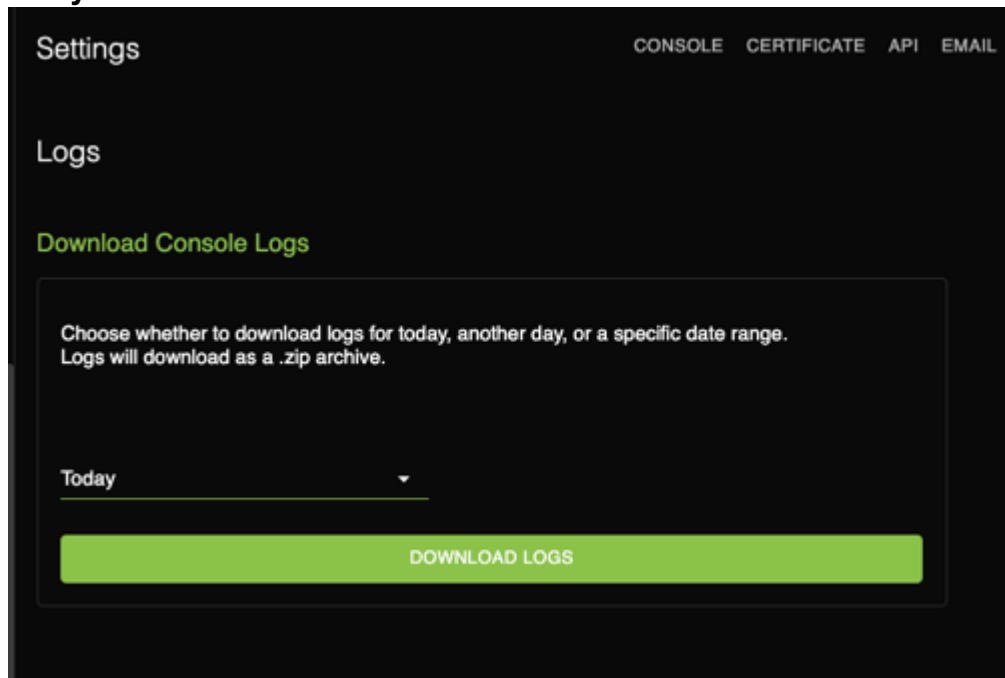
The Console logs are available to download for tracking or troubleshooting purposes.

Log files

You can download log files for the Discovery Console for OT.

To download these logs, do the following.

- In the Console, go to the Settings page.
- On the Settings page, select the **Log** tab.
- In the drop-down field, select one of the date settings.
 - **Today**



- **Date range**

○ **Custom date**

- Select **Download Logs** to download a compressed zip file of all log files.

Sensor log files

The Console has an early access capability for retrieving Sensor logs. Currently, accessing these logs requires deep technical expertise of the system. Leave this feature inactive unless directed to enable from Customer Service and Support.

If you have questions or need assistance, [contact Customer Service and Support.](#) 

Discovery Sensor for Operational Technology (OT)

Use the Discovery Sensor for Operational Technology (OT) application to discover and query devices in the Operational Technology environment.

Get started

Use the links in the Related Topics section to explore, configure, and learn more about the ServiceNow Discovery Sensor for Operational Technology (OT).

Log files

To review files on your Sensor and access logs for troubleshooting purposes, you can SSH from another machine that has network access to the Sensor. If you have to authenticate, use the default credentials. Refer to [Configure the Discovery Sensor for OT](#) for the credentials.

Explore the Discovery Sensor for Operational Technology (OT)

The Discovery Sensor for OT provides you with enhanced scanning and query functionality to manage your assets in the OT environment.

Discovery Sensor for OT overview

This section provides an overview of the Discovery Sensor for OT and its integration with the Discovery Console for OT. For more information, see [Discovery Console for Operational Technology \(OT\)](#).

Sensors on the Discovery Console for OT

The Appliance page displays a list of all Sensors and Collectors that are associated with a Discovery Console for OT.

Appliances records

The Discovery Sensor for OT is listed on the Appliances page separately from the Collector. If you select the Sensor name from the list, you can open that Sensor record. You can perform the same actions with the Sensor as you would with the Collector. However, Collectors aren't registered to the Console. For more information, see [Appliances page](#) and [Edit an Appliance](#).

Configure the Discovery Sensor for OT

Configuring the Discovery Sensor for OT provides discovery of all assets in your OT environment. The Sensor requires a Linux operating system that is installed either as a virtual machine or on a Bare-metal computer that is x86.

Discovery Sensor for OT System requirements

System Requirements

Component	System Requirements
Discovery Sensor for OT	• 16 GB RAM • 100 GB Hard drive • 2 CPUs • 2 virtual NIC cards

Workflow

Review the steps in the Sensor installation process from the table.

Discovery Sensor for OT Installation Workflow

Task	Description
Navigate to the Download & Deploy OT Discovery page.	In the ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page and select Download & Deploy OT Discovery.
The Downloads page opens.	Download the Discovery Sensor for OT package.
EULA Agreement	Ready the EULA appears on the Downloads page. Accept the EULA by checking the box next to Agree .
ISO image	Unzip the Sensor package. The ISO image is included in the Sensor package.
Create a virtual machine.	Select Other Linux 64-bit as the OS.
CD/DVD	Attach the Sensor ISO to the CD/DVD to boot the VM.
Run the installation.	Follow the installation steps in Install the Discovery Sensor for OT .
Register the Sensor	Register the Sensor with the DMI and Console. This confirms that the Console and Sensor can communicate with each other. For more information, see Register the Discovery Sensor for OT for more information.

Install the Discovery Sensor for OT

Download the Discovery Sensor for OT package and install the ISO image. Then install the Discovery Sensor for OT.

Before you begin

Role required: admin

About this task

You can register the Sensor after you have installed the OT Discovery Console and system. Before you can register a Sensor to the Console, you must confirm that you have completed the following.

- From the Downloads page, download the Sensor package; the Sensor ISO file is in the same package.
- Install the ISO image.
- Determine if you're using the ISO as a Virtual Machine (VM) or are installing the ISO on hardware. If you're using the ISO as a VM, you can use any of the following VMs.
 - VWare
 - Hyper-V
 - Proxmox

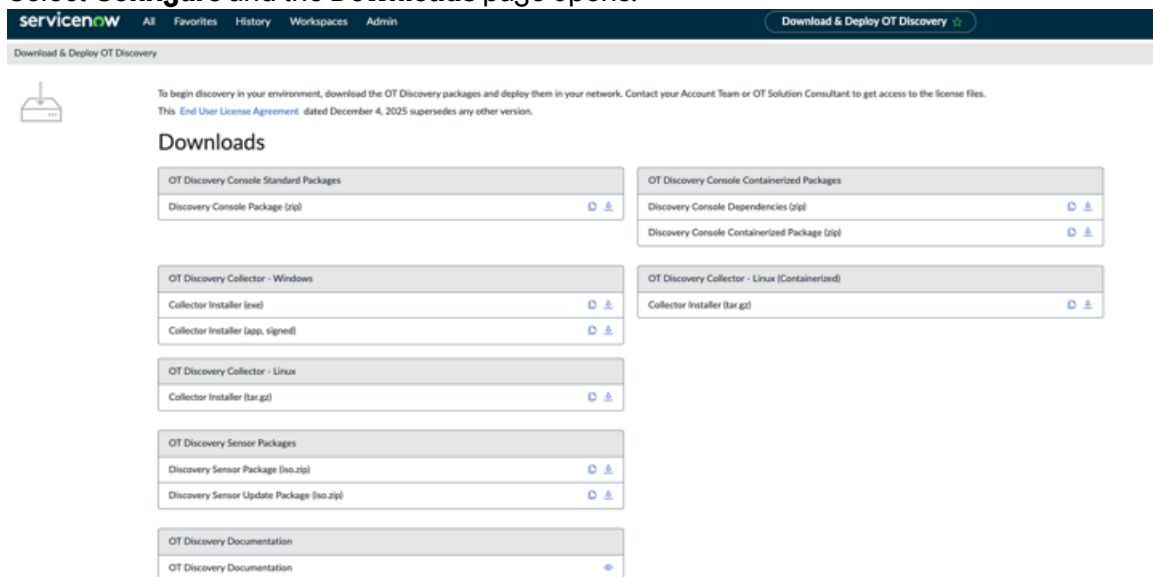
- Linux KVM

If you choose to install the ISO on hardware through BareMetal, you must use a tool to create a USB ISO installer.

- You must open both the Console and the DMI interfaces to complete the Sensor registration.

Procedure

1. On your instance, navigate to the [Service Graph Connector for ServiceNow Operational Technology \(OT\) Discovery](#) Guided Setup page.
2. Select the **Get Started**.
The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.



Note: Read the End User License Agreement (EULA) carefully and then check **Agree**.

5. Download the Discovery Sensor for OT installation and deployment package.
6. Unzip the Sensor package.
The ISO image is included in the Sensor package.
7. Create the virtual machine for the Discovery Sensor for OT.
8. Install the Discovery Sensor for OT.
9. Select the default answers for all prompts.
10. Upload the ISO image to your virtualization platform.
11. Create the hardware NICs which the VM uses to communicate with the Sensor.

Note: The following images are examples specific to an ESXi 8.0 U2 virtual machine.

Edit settings - core-image-minimal-genericx86-64-20250610181459 (ESXi 8.0 U2 virtual machine)

Virtual Hardware **VM Options**

> General Options VM Name: core-image-minimal-genericx86-64-202506101814

> VMware Remote Console Options ☒ Lock the guest operating system when the last remote user disconnects

> VMware Tools Expand for VMware Tools settings

> Power management Expand for power management settings

Firmware Choose which firmware should be used to boot the virtual machine:
EFI

Enable UEFI secure boot ☐ Whether or not to enable UEFI secure boot for this VM

Boot Delay Whenever the virtual machine is powered on or reset, delay boot by
0 milliseconds

Force BIOS setup ☐ The next time the virtual machine boots, force entry into the BIOS setup screen.

Failed Boot Recovery ☐ When the virtual machine fails to find a boot device, automatically retry boot after
10 seconds

CANCEL **SAVE**

Note: For communications to work between Discovery components, two network adapters should be connected on the VM.

Edit settings - core-image-minimal-genericx86-64-20250610181459 (ESXi 8.0 U2 virtual machine)

Virtual Hardware **VM Options**

Add hard disk **Add network adapter** **Add other device**

> CPU 2

> Memory 8 GB

> Hard disk 1 16 GB

> SCSI Controller 0 VMware Paravirtual

SATA Controller 0

USB controller 1 USB 2.0

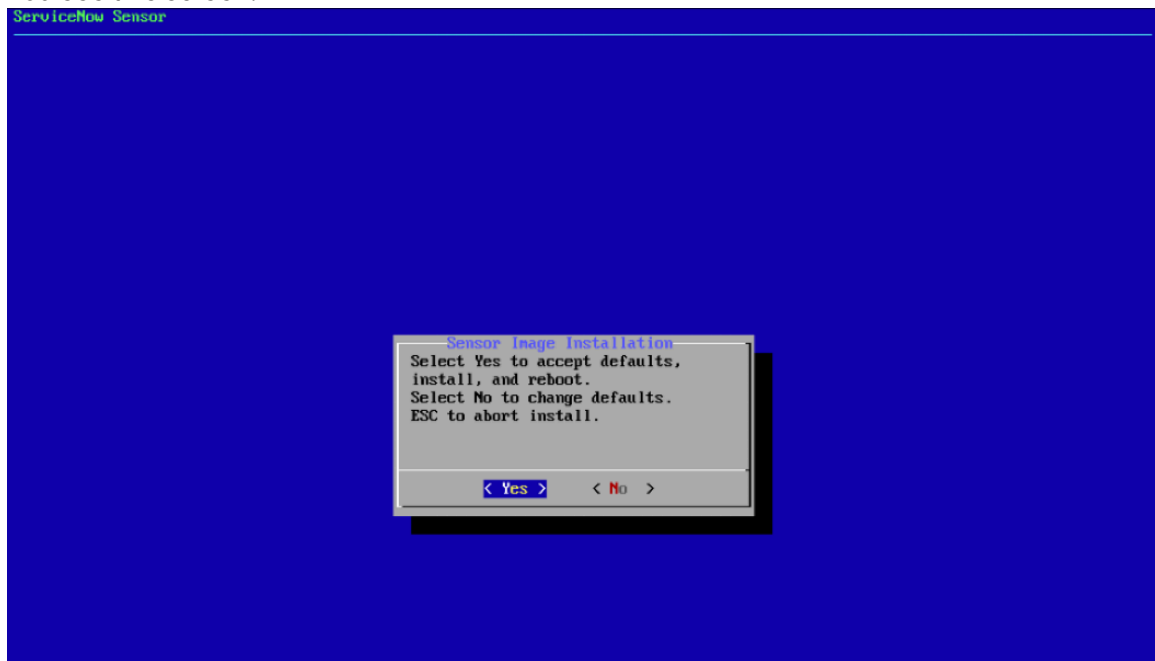
> Network Adapter 1 VM Network ☒ Connect

> Network Adapter 2 VM Network ☒ Connect

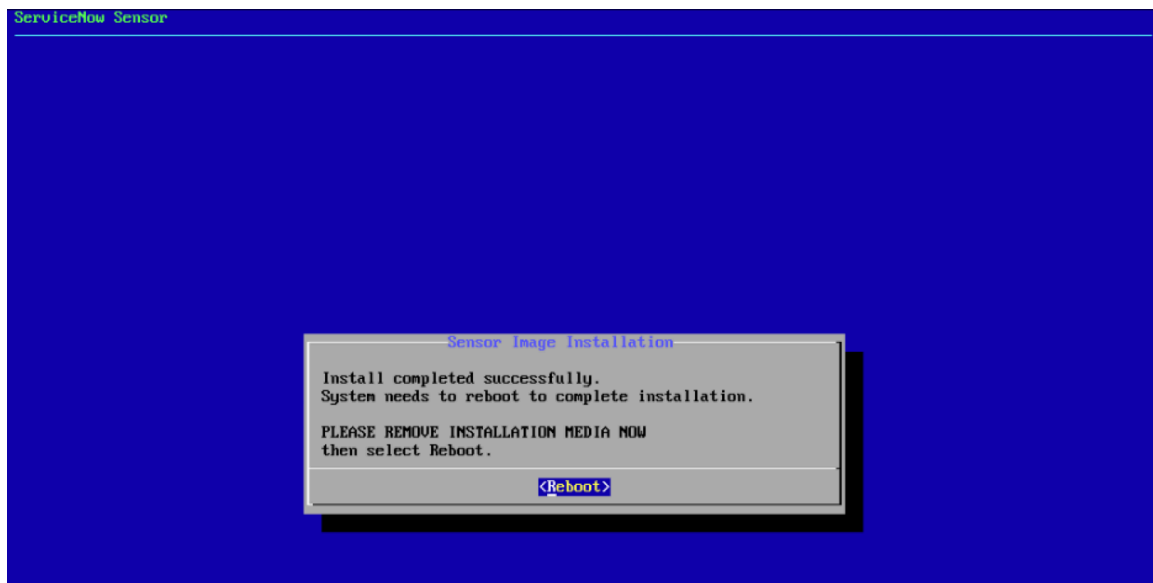
> CD/DVD Drive 1 Datastore ISO file ☒ Connect

- Note:** For other VM options, confirm that EFI is selected (and not BIOS) as the Firmware and that the "Enable Secure Boot" flag is not selected.

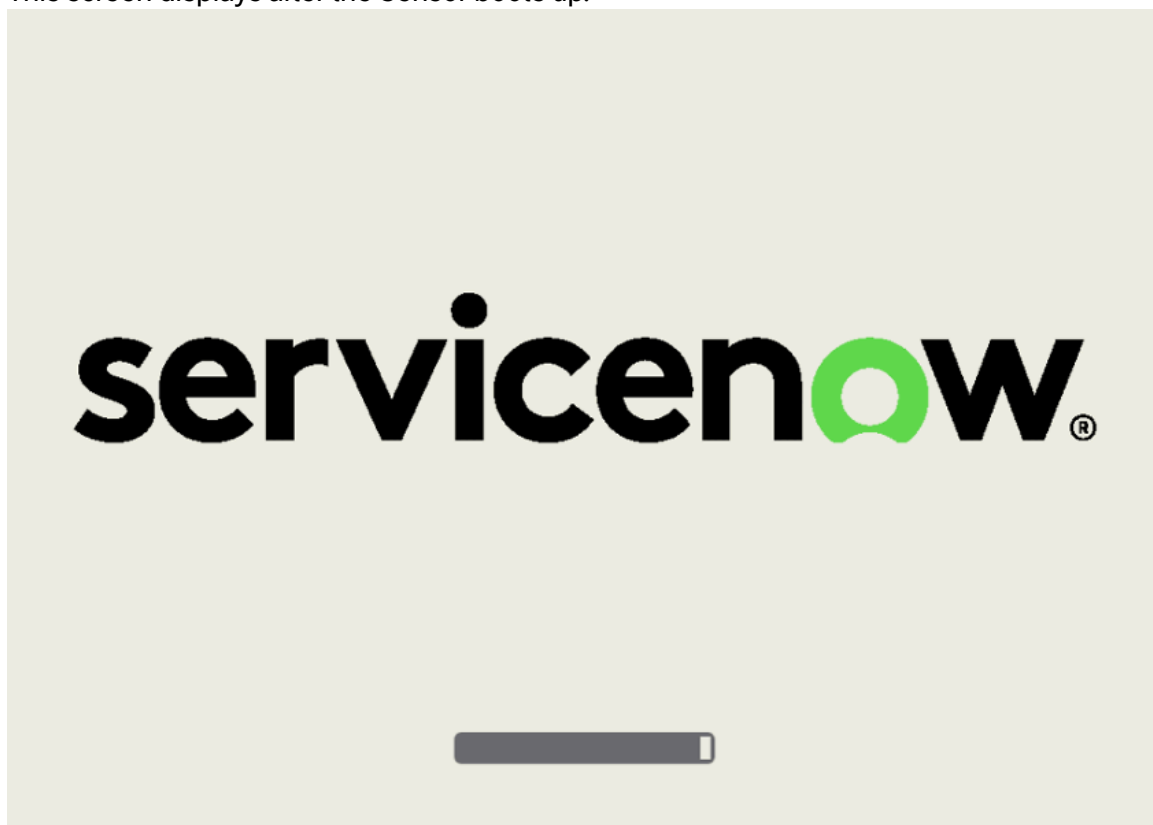
12. Install the ISO image.
13. After installing, when alerted, remove any install media.
The alert message is: "System needs to reboot to complete installation. Please remove all install media and once complete press any key to reboot."
14. Reboot the system.
15. After removing any install media, the install process starts for the Sensor.
16. Create the virtual machine for the Sensor.
17. Select the OS as **Other Linux 64-bit**.
18. Attach the Sensor ISO to the CD/DVD to boot the VM.
19. Create 2 hardware NICs specifically for the VM.
20. For other VM options, confirm that EFI is selected (and not BIOS) as the Firmware and that the "Enable Secure Boot" flag is not selected.
21. Assign a minimum of 8 GB RAM and 60 GB HDD for the installation.
22. Power on the VM and the install starts.
You see this screen:



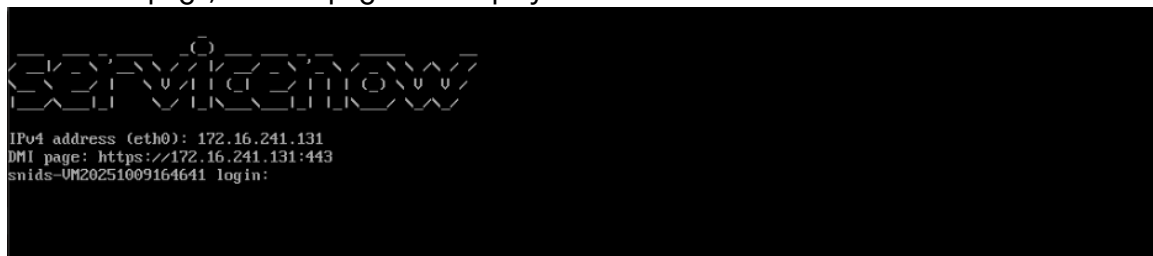
23. Select **Yes** to start the install.
24. Once the install is complete, select **Enter** to reboot the VM.



This screen displays after the Sensor boots up.



25. On the VM page, the DMI page URL displays.



26. Use this URL to log in to the DMI and register your Discovery Sensor for OT to the Console. For more information, see [Register the Discovery Sensor for OT](#).

What to do next

[Register the Discovery Sensor for OT](#)

Register the Discovery Sensor for OT

When you have installed the Discovery Console for OT and the Discovery Sensor for OT, register the Sensor to the Console with the Console's Device Management Interface (DMI).

Before you begin

Role required: admin

About this task

Confirm you that you have installed the Sensor. You must register the Sensor to the Console with the DMI. The DMI is a web-based interface that lets you configure and register the Sensor with the Console. For more information on the DMI, see [Device Management Interface](#). Registering the Sensor confirms it can communicate with the Console.

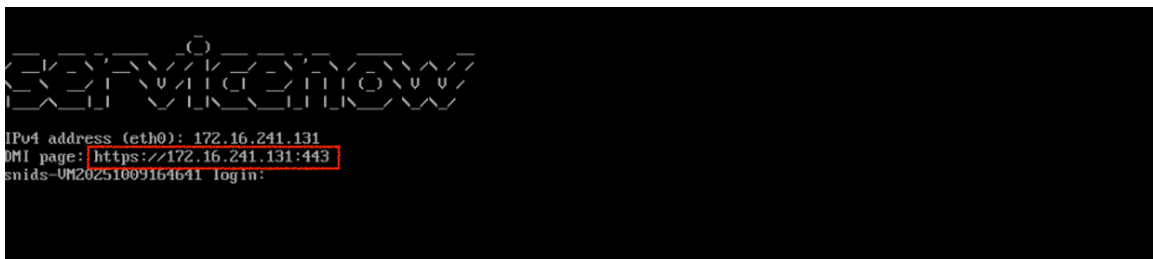
Procedure

1. Access the DMI for a Discovery Sensor for OT by opening a browser and entering the URL displayed on the screen when the Sensor is installed and boots up.

Note: Currently, there isn't a serial number portion since there's no active hardware. These input steps are still valid. But the [serial number] is likely to be the Sensor name at the time of its creation. This is an example of how to find the URL for the DMI. Your IP address will be different from this example:

```
https://[device type]-[serial number] with
either .local:443 or .[domain name]:443
```

Be sure to make a note of the DMI URL displayed after the Sensor is installed. You can use this URL for the DMI. This image shows the DMI URL as `https://172.16.241.131:443`.



2. In the DMI, log in using your credentials.

- DMI (Web Interface):
 - Username: admin
 - Password: password
- SSH login:
 - Username: serviceadmin
 - Password: devpassword

Note: After the initial log in is completed, the DMI prompts you to change the password.

3. In a separate tab or browser, log in to the Discovery Console for OT.
4. In the Console, navigate to **Appliances > Certificates**.
5. Under Sensor Credentials, select the **Generate Bundle**.
In the prompt window, select **Generate Bundle** again.
6. The bundle generates and downloads to your designated download folder.
7. Switch back to the DMI.
8. In the DMI, navigate to **Console > Credentials**.
9. Select **Bundle File Input** and from this window, select the generated Sensor bundle.
10. Select **Upload Credentials Bundle** to upload the Sensor bundle to the DMI.
After the bundle is uploaded, the **Certificate Update Logs** appears and confirms the completed process.
11. The DMI automatically extracts the certificate from the bundle and registers the Sensor.
12. From the DMI menu, select the **Network** tab.
13. Select the **Edit** button.
14. Select an IP Address or Hostname for the Console endpoint and enter a valid value.
Enter a valid Gateway IP Address.
15. Select **Save & Deploy**.
16. Navigate back to the **Console** tab and select the **Register** button.
17. In the Console, confirm that the Sensor is online.
The device briefly shows online and then offline. Then it shows a steady online status in the Console.

Result

The Sensor and the Console can now communicate and generate queries.

Device Management Interface

The Device Management Interface (DMI) is a web-based interface where you configure and register a Discovery Sensor for OT to the Discovery Console for OT.

DMI overview

With the DMI, registering a Sensor enables the Sensor to communicate with the Discovery Console for OT. By registering the Sensor, you're ready to start using the Console.

Note: The Console and the DMI are separate web-based interfaces that you access with an HTTPS web address. Open both interfaces when registering the Sensor. During the first log in to the DMI, the username `admin` and the password `devpassword` are provided.

Once the Console is deployed and you have registered the Sensor, you can create these necessary components on the Console to discover assets in your environment.

- Site
- Network Zone
- Auto Query
- Quick Scan

For more information about these Console features, see [Discovery Console for Operational Technology \(OT\)](#).

DMI pages

The following sections describe the pages available on the DMI.

Device

The Device page includes a summary of the basic configuration information for the Sensor. This page includes details about the Sensor's name, type, description, serial number, firmware version, build date, model, and revision.

On the Device page, you can edit the Sensor name. If you change the name before you register the Sensor, the updated name appears in the Console. Otherwise, if you change the name after registering the Sensor, you must update the Sensor name in the Console itself.

Network

The Network page includes a diagram of the Sensor and information about its connection to the Console, management interface, and bridge or span interface. You can edit the information on this page as needed when registering the Sensor.

Console

The Console page enables you to register the Sensor with the Console. If needed, you can edit the Console endpoint and Console gateway from this page. Selecting the **Edit Settings** button redirects you to the Network page, where you can make your changes. After you register the Sensor with the Console, the Sensor appears in the Console on the Sensors page.

Location

The Location page includes the following fields that describe the location of the Sensor.

- Latitude
- Longitude
- Description of the physical location

You can add or change the location information for a Sensor by selecting the **Edit** button.

Password

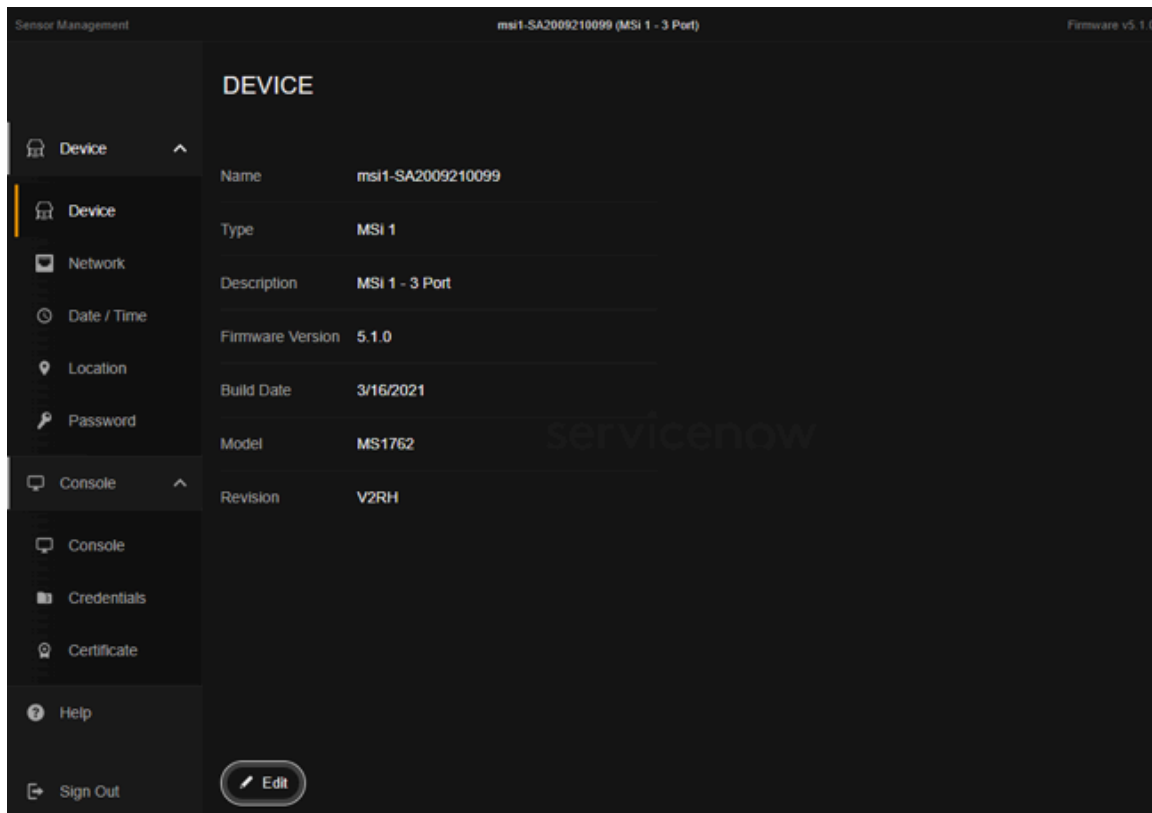
The Password page provides the option to update the password of the DMI. You can change the password by selecting **Edit** and entering the updated password.

Certificate

The Certificate page enables you to upload a certificate downloaded from the Discovery Console for OT. This certificate is needed for registering the Sensor with the Discovery Console for OT.

Help

The Help page includes information about keyboard shortcuts related to the DMI.



Deregister a Discovery Sensor for OT

Deregister a Discovery Sensor for OT from the Discovery Console for OT that is no longer available on your system.

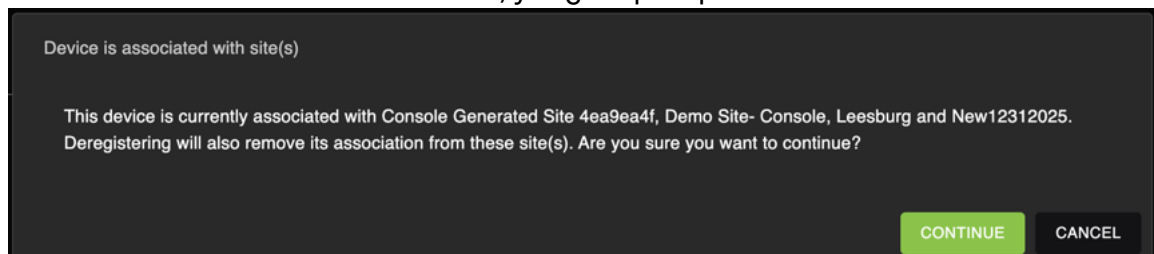
Before you begin

Role required: admin

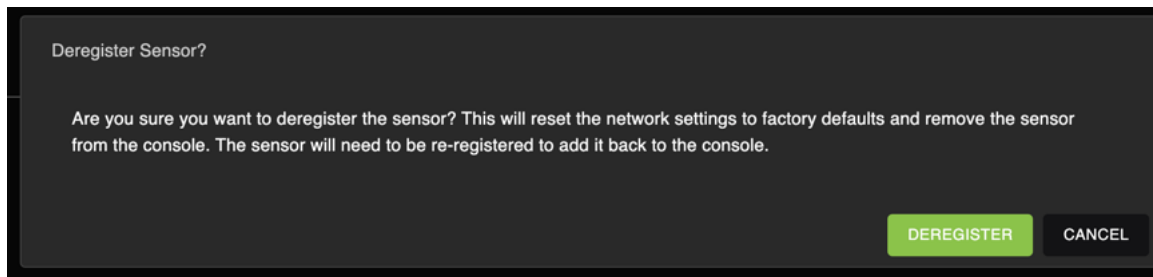
Procedure

1. In the Console, navigate to the Appliances page.
2. From the list, select the Sensor that you want to deregister.
The Sensor record opens.
3. In the record, select the Actions icon.
4. Select **Deregister** from the menu.

When the Sensor is associated to a Site, you get a prompt.



5. If you select Continue in this window, you receive a prompt:



6. If you still intend to deregister the Sensor, select the **Deregister** button in this window.

Result

The Sensor is deregistered, and the Sensor is reset to the default network configuration, which is the DHCP with the link-local fallback.

Remove a lost Sensor

Remove a Sensor that no longer functions or is otherwise reported as having a lost connection from the Discovery Console for OT.

Before you begin

Role required: admin

Procedure

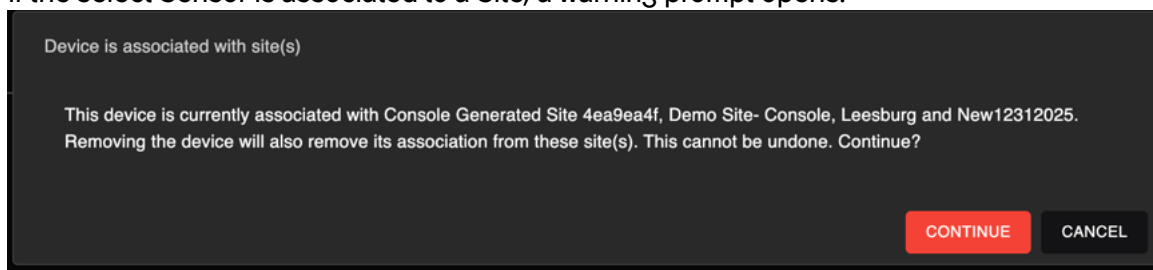
1. Navigate to the **Appliances** page.
2. From the list, under the Name column, select the Sensor that you want to remove.

⚠ Danger: Removing Sensors in the OT environment may require working in environments with dangerous voltages, moving parts, and other safety hazards. Sensors should only be removed by persons with proper electrical and workplace safety training.

3. The Sensor record opens for the selected appliance.
4. In the record, select the Action button.
5. From the menu, select **Remove Device from Console**.

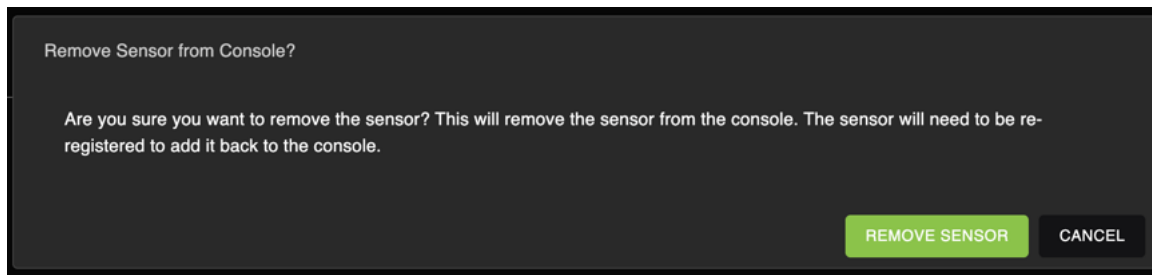
i Note: The **Remove Device from Console** option is only available in the drop-down if the Device Status is **Connection Lost**.

6. If the select Sensor is associated to a Site, a warning prompt opens.



Removing a Sensor that is associated to a Site can't be undone.

7. If you still intend to remove the Sensor, select **Continue**.



8. Select the **Remove Sensor** button to complete the removal.

Result

The Sensor is no longer displayed on the Discovery Sensor for OT list page. Existing network connections associated with the Sensor remain in the system for historical purposes.

i Important: If you remove a lost Sensor from the Console, it may still be powered on and operating at its installed location. Verify that the Sensor is properly powered down and removed from the field after removing them from the Console. If a lost Sensor is found to be operational after having been removed and must be reinstalled on the network, you must contact the Technical Support team for assistance in reconfiguring the Sensor.

Operational Technology Discovery Collector

Use the OT Discovery Collector component to discover devices the Discovery Sensor for OT can't reach in the OT environment.

Get started

Use the links in the Related Topics section to explore, configure, and use the OT Discovery Collector.

Explore the Operational Technology Discovery Collector

The OT Discovery Collector provides you with enhanced features to create an inventory of your assets in your OT environment.

OT Discovery Collector overview

The OT Discovery Collector is a lightweight software application that is used to discover devices within segments of the OT network where a Sensor can't reach. It is deployed deep within the network zones in your OT environment. The Collector delivers native protocol support without requiring any appliance, making it fast to implement and easy to scale.

Appliances records

The OT Discovery Collector is listed on the Appliances page separately from the Discovery Sensor for OT. If you select the Collector name from the list, you can open that Collector record. You can perform the same actions with the Collector as you would with the Sensor. However, you aren't required to register a Collector to the Discovery Console for OT. For more information see, [Appliances page](#) and [Edit an Appliance](#)

What to explore next

For more information about the OT Discovery Collector or to get help with the application, see:

- [Configure the OT Discovery Collector](#)
- [Contact Customer Service and Support](#) 

Configure the OT Discovery Collector

The OT Discovery Collector is an application that you can install on a Windows or Linux system.

Collector Credentials

Depending on how you have deployed the Console, you may have to manually edit the `hostname` value in the `config.json` file to validate the Collector's credentials. If you install an offline Console or install into cloud environments, the `hostname` value may not be correct. For the OT Discovery Collector, the `hostname` needs to be set to the Console hosts external/network IP address. It is important to check this setting and adjust it as needed.

Note: You can now download and install Containerized Collector packages. For a Windows OS machine, be sure to select the compatible Collector OS. For more information, see [Air-gapped networks and OT Discovery installation](#).

Collector minimum system requirements

The OT Discovery Collector can be installed and run on either a Windows OS or a Linux OS.

Component Operating System	Minimum System Requirements
Windows	The OT Discovery Collector installation is compatible with Windows 10 or Windows 11 systems. The required Windows (10 or 11) environment for the OT Discovery Collector is x86_64. ARM or Apple Silicon devices aren't supported. For more information, see Install the OT Discovery Collector on a Windows system.
Linux	For more information, see Install OT Discovery Collector on a Linux system.

Install the OT Discovery Collector on a Windows system

Install the OT Discovery Collector on a Windows system. The OT Discovery Collector installation is compatible on Windows 10 or Windows 11 systems.

Before you begin

The required Windows (10 or 11) environment for the OT Discovery Collector is x86_64. No ARM/Apple Silicon devices are supported.

Role required: admin

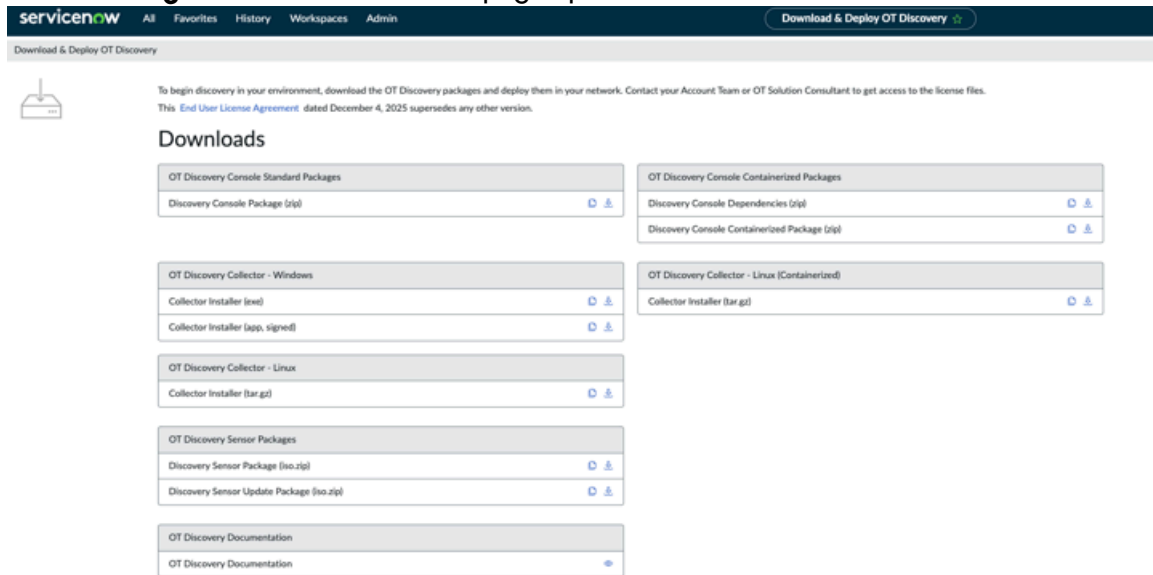
Note: You can now download and install Containerized Collector packages. For a Windows OS machine, be sure to select the compatible Collector OS. For more information, see [Air-gapped networks and OT Discovery installation](#).

Procedure

1. On your instance, navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup page.
2. Select the **Get Started**.
The **Download & Deploy OT Discovery** page opens.

3. In the first section of the setup, select **Download & Deploy OT Discovery**.

4. Select **Configure** and the **Downloads** page opens.



Note: Read the End User License Agreement (EULA) carefully and then check **Agree**.

5. Download the OT Discovery Collector installation and deployment package for Windows.

6. Install the Collector on the Discovery Console for OT you intend to use.

7. On the Discovery Console for OT, navigate to the **Sensors > Certificates >** page.

8. To generate the OT Discovery Collector credentials you need, from the list under the Bundle Password section, select the **Generate Password** button.

9. Select the radio button next to the desired **Bundle Format**.

The recommended format is ZIP.

10. Select the **Generate Bundle** button.

The Generate OT Discovery Collector Credential Bundle window opens.

11. Select the **Generate Bundle** button in this window.

The ServiceNow_OT_Discovery_Collector_Windows bundle zip file is downloaded to your machine.

12. Extract the ServiceNow_OT_Discovery_Collector_Windows.zip file.

The zip file contains a config.json file and a cert folder. The cert folder contains the following files:

- ca_root_certificate.pem
- client.device.rabbit.pem
- client.device.rabbit.privatekey.pem

13. Navigate to the

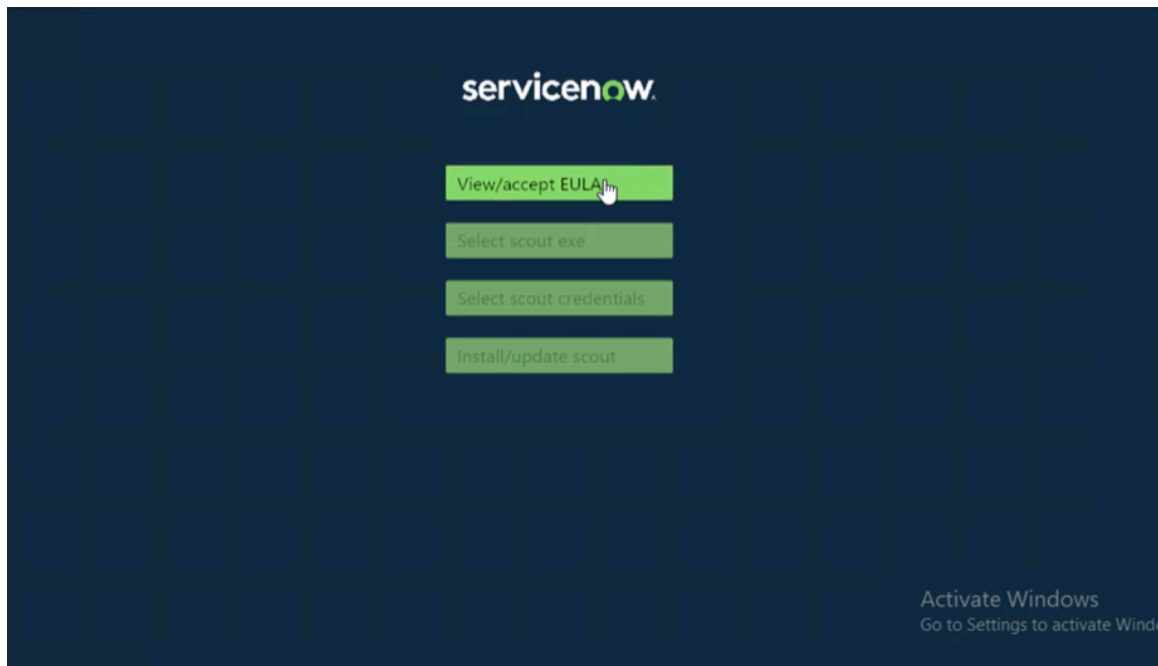
ServiceNow_OT_Discovery_Collector_Windows_Installer_[timestamp] folder.

14. In this folder, select and hold the right key on the

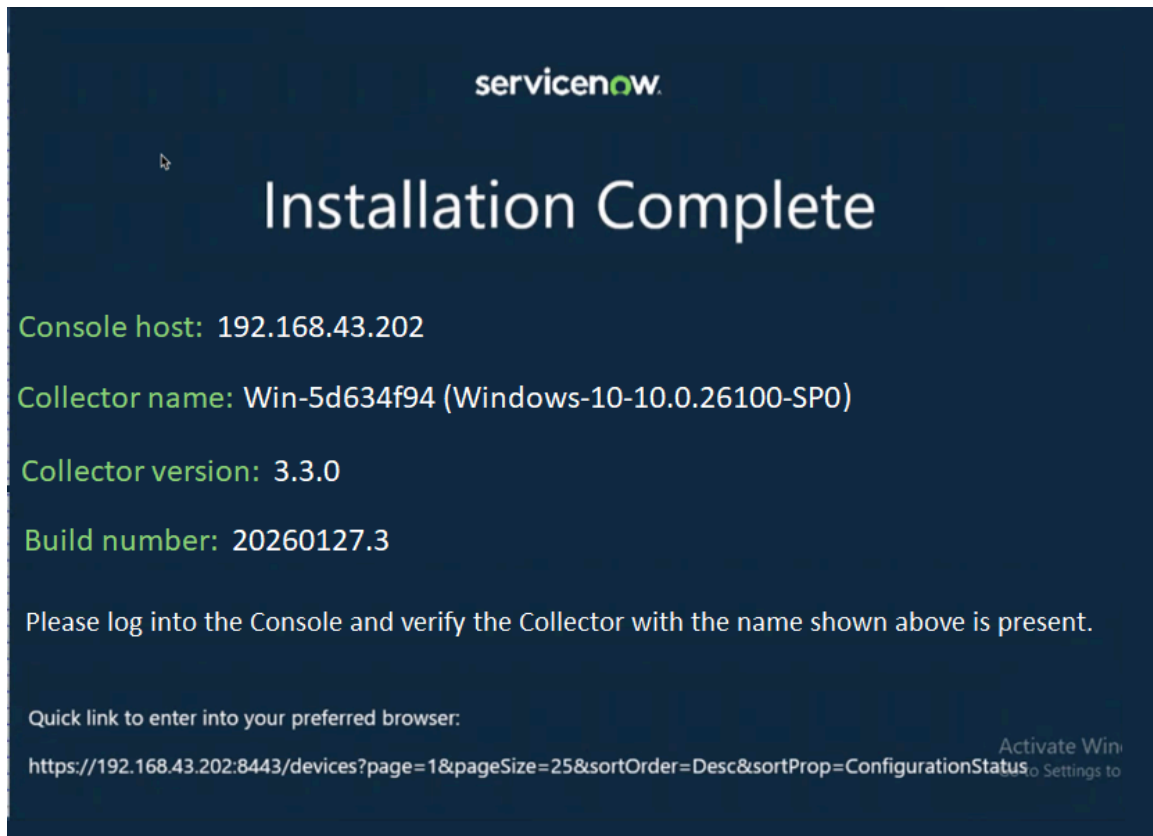
ServiceNow_OT_Discovery_Collector_Windows_Installer file and select **Run as Administrator**.

15. When prompted, select **Yes** to enable this app to change to your computer.

The ServiceNow OT Discovery Collector Installer window starts the installation.



- 16.** Select the **View/accept EULA** button to accept the End User License Agreement (EULA). Read the EULA carefully. If you don't agree to the EULA, or skip this step, the installation is canceled.
When you accept the EULA, a dialog window pops up.
- 17.** In the dialog window, select the `SNDiscoveryCollector_install_windows` file and select **OK**.
- 18.** Select the **Select *OT Discovery Collector* Credentials** button.
After you select this button, a dialog window opens.
- 19.** In the window, select the `collectorBundle` file and select **OK**.
- 20.** Select the **Install/Update Collector** button on the installation screen.
When complete, the ServiceNow OT Discovery Collector Installer window displays **Installation Complete**.



21. Navigate to your local disk program files folder, so that you can see the SNDISCOVERYCOLLECTOR folder is present.
22. **Optional:** Navigate back to the Download & Deploy OT Discovery page and select **Mark as complete**.

Result

In the Discovery Console for OT window, the OT Discovery Collector appears on the Discovery Sensor for OT screen.

The OT Discovery Collector is installed on your Discovery Console.

What to do next

To update the OT Discovery Collector version, do the following steps.

1. Re-run the installer.
2. Select the latest version of the OT Discovery Collector.
3. Use the same credentials again.
4. Select the **Install/Update OT Discovery Collector** button.

The updated version is installed.

Install OT Discovery Collector on a Linux system

Install the OT Discovery Collector on a Linux system.

Before you begin

- SCP the `linuxCollectorinstaller_[version number]_[build number].tar.gz` over to the Linux system.

Note: An example of the file name format is `linuxCollectorinstaller_3.3.1_20250917.1.tar.gz`.

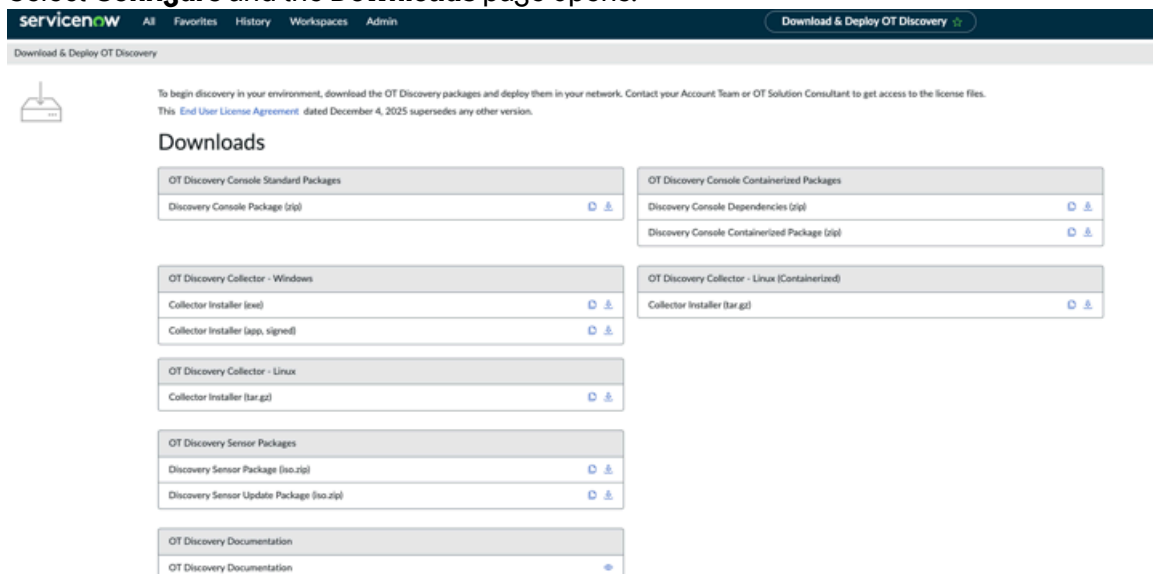
- SCP the `CollectorBundle` file you generated and downloaded from the Discovery Console to the Linux system.
- To go into OT Discovery Collector Linux host, use `ssh`.
- Use `su` or `sudo -s` to switch to the root user.

Role required: admin

Note: You can now download and install Containerized Collector packages. For a Windows OS machine, be sure to select the compatible Collector OS. For more information, see [Air-gapped networks and OT Discovery installation](#).

Procedure

1. On your instance, navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup page.
2. Select the **Get Started**.
The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.



Note: Read the End User License Agreement (EULA) carefully and then check **Agree**.

5. Download the OT Discovery Collector installation and deployment package for Linux.
6. Install the Collector on the Discovery Console for OT you intend to use.
7. On a RHEL-based distribution, install `tar`.

```
sudo dnf install -y tar
```

8. On all Linux distributions, run the following command:

```
tar -xvf linuxCollectorinstaller_[version number]_[build number].tar.gz
```

9. Copy the CollectorBundle file into the CollectorInstaller directory.

```
chmod +x Collector-init.sh
```

```
./Collector-init.sh
```

10. When the script starts, the system locates the pdf version of the EULA.

When prompted to accept the EULA, enter Y for yes.

11. After the script completes successfully, the OT Discovery Collector can be seen in the console.

To check the service status, run this command: `systemctl status SNDiscoveryCollector`. If you would like to view the journal output for the service to troubleshoot issues, as the root user you can run `journalctl -f -a -u SNDiscoveryCollector`.

Result

After the script completes successfully, the OT Discovery Collector can now be seen in the console.

To check the service status, run this command:

```
systemctl status SNDiscoveryCollector
```

If you would like to view the journal output for the service (usually as a troubleshooting measure), as the root user you can run:

```
journalctl -f -a -u SNDiscoveryCollector
```

Use the OT Discovery Collector

When your OT Discovery Collector stops or loses power use the next task specific to your OS to restart it.

Helpful Tasks

Use the links in the Related Topics section to do the tasks needed when your OT Discovery Collector stops or loses power.

- [Restart OT Discovery Collector on a Windows system](#)
- [Restart OT Discovery Collector on a Linux system](#)

Restart OT Discovery Collector on a Windows system

Perform manual restart of the OT Discovery Collector when its configuration file has been refreshed, or if it is unstable. You can perform manual restart only on Collectors installed in a Windows environment and for Linux-based agents that use `systemd`.

Before you begin

Role required: admin

Procedure

1. On a windows system, navigate to the host where OT Discovery Collector is running.
2. Open the Services dialog in Windows.
3. Select SNDiscoveryCollectors.
4. Select **Restart the service**.

Result

OT Discovery Collector restart in the Windows environment.

Restart OT Discovery Collector on a Linux system

Perform manual restart of Collector when its configuration file has been refreshed, or if the OT Discovery Collector is unstable. You can perform manual restart only on the Collectors installed in a Windows environment and for Linux-based agents that use `systemd`.

Before you begin

Role required: admin

Procedure

1. Use SSH to access the Linux host.
2. Use `sudo` or `su` to run the following command with root permissions.

```
systemctl restart SNDiscoveryCollectors
```

Result

OT Discovery Collector restarts in the Linux environment.

Service Graph Connector for ServiceNow Operational Technology (OT) Discovery

The Service Graph Connector for ServiceNow Operational Technology (OT) Discovery (SGC) imports data from a connected Operational Technology Discovery OT Discovery environment and leverages the Integration Hub ETL framework.

Use the links in the Related Topics section, to explore and configure the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery.

Troubleshooting

If you have any errors or difficulties while using the Service Graph Connector, [Contact Customer Service and Support](#). 

Explore the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery

The Service Graph Connector for ServiceNow Operational Technology (OT) Discovery imports data from a connected Operational Technology (OT) Discovery environment and leverages the Integration Hub ETL framework.

What to do next

Go through each step to install and setup the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery (SGC).

Service Graph Connector for ServiceNow Operational Technology (OT) Discovery prerequisites and settings

During set up of the Discovery Console for OT, review and confirm you have the following settings.

Dependencies and requirements

Confirm you have these settings and then follow the Discovery Console for OT Guided Setup.

Dependencies and requirements:

- The [Industrial Core](#)  plugin.
- The [ISA Equipment Model](#)  store app with a minimum version of 1.0.11.
- 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.

Install the Service Graph Connector for ServiceNow Operational Technology Discovery

Install the Service Graph Connector for ServiceNow Operational Technology Discovery from the ServiceNow Store.

Before you begin

Role required: admin

Procedure

1. In the ServiceNow Store, navigate to and select **Get** on the Service Graph Connector for OT Discovery store page to entitle the integration to one or more ServiceNow instances.
2. Once entitled, log into your instance.
3. Navigate to **System Applications > All Available Applications > All**.
4. Locate the Service Graph Connector for ServiceNow OT Discovery and select **Install**.

Result

The Service Graph Connector for ServiceNow Store OT Discovery application is installed on your instance.

What to do next

From your ServiceNow instance, navigate the **All** menu to find the Service Graph Connector for ServiceNow Operational Technology Discovery Guided Setup. This guides you through all the mandatory and optional steps to setting up the Service Graph Connector for OT Discovery.

Service Graph Connector for ServiceNow OT Discovery Guided Setup

Use the Guided Setup for the Service Graph Connector for ServiceNow OT Discovery to lead you through the installation, connection, configuration, and integration steps for the OT Discovery environment.

Before you begin

Review the [Service Graph Connector for ServiceNow Operational Technology \(OT\) Discovery prerequisites and settings](#) section before beginning.

Role required: admin

Procedure

1. From your ServiceNow instance, navigate the **All** menu.
2. Enter **Service Graph Connector** into the filter and scroll down the menu to find **ServiceNow OT Discovery**.
3. Select **Setup**.
4. The **Service Graph Connector for ServiceNow OT Discovery Guided Setup** page opens.
5. On the **Guided Setup** page, select **Get started**.
This opens the page with each task for downloading the OT devices and steps to configure connections, integrations, and imports for the Service Graph Connector.
6. In the first section, select **Download & Deploy OT Discovery**.
This opens the **Download & Deploy OT Discovery** page.
7. Select **Configure**.
8. Read the EULA and then download the packages for the Console, Sensor, and Collector.
9. Choose the OT Discovery Collector OS package that matches your machine's OS.

Note: If you have a closed network, download the Sensor package and the containerized versions of the Console and Collector packages. When ready, install the Console first, install the Sensor after that and, finally, install the Collector. For more information, see [Air-gapped networks and OT Discovery installation](#).

10. Return to the previous page and select **Mark as complete**.
11. Go back to the **Service Graph Connector Guided Setup** page.
12. The next section is **Configure table permissions**.

Note: Setting the table permissions allows you to have multiple connections across multiple consoles. This depends on your deployment choice of the Discovery Console for OT.

- a. In the **Configure table permissions** section, select **Scheduled data import**.
This opens the **Configure table permissions** page.
- b. Next to the **Scheduled data import** task, select **Configure**.
- c. The **Scheduled data import table** opens.
- d. In the table, select the **Application Access** tab.
- e. Confirm that the **Can Read**, **Can Create**, and **Can Update** options are checked.
- f. Select **Update**.
- g. Return to the **Configure table permissions** page and select **Mark as complete** next to the **Scheduled data import** task.
- h. Select **Configure** next to the **Data source** task.
- i. The **Data source table** displays.

- j. Select the **Application Access** tab.
- k. Confirm that Can Read, Can Create, and Can Update options are checked.
- l. Select **Update** or **Save**,
- m. Return to the Configure table permissions page and select **Mark as complete** next to the **Data source** task.
- n. Return to the Guided Setup page.

i Note: These settings give you flexibility in how you setup your system. The Service Graph Connector for ServiceNow OT Discovery supports multiple-connections to multiple consoles. This depends on the deployment choice made for the Consoles. These settings give you the ability to create multiple data source objects, console objects, and multiple schedules from which to pull data.

What to do next

The next step in the Guided Setup is [Configure the OT Discovery connections & credentials](#).

Configure the OT Discovery connections & credentials

Configure the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery authentication credentials and configuration used to connect to the ServiceNow OT Discovery devices.

Before you begin

Role required: admin

i Note: It's recommended that you switch to the application scope to Service Graph Connector for ServiceNow Operational Technology (OT) Discovery.

Procedure

1. Confirm that the application scope is set to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery by using the application picker.
2. Under **Configure the connection** section only configuring the MID Server is optional.

i Note: The MID Server is required when the console can't be reached from the internet. If the console is reachable to the ServiceNow instance then MID Server is not needed.

3. Download and install the MID Server on the host machine, test the connection, and then validate the MID Server.
Configure the MID Server using the MID Server Guided Setup.

The MID Server access is a secure proxy between the ServiceNow Instance and the Console, allowing ServiceNow to schedule jobs and make REST calls into the environment to pull various pieces of information such as Assets, installed software, and so on. Without the MID Server, ServiceNow can't initiate direct communication if the Discovery Console is not reachable from the ServiceNow Instance

4. Use the MID Server certificate check policies link to review the policies.

i Note: Enable/Disable the required security policies for the MID Server based on the network configuration.

5. Next to the **Configure the OT Discovery Connection & Credentials** task, select **Configure**.

Note: Depending on your ServiceNow version, you're directed to Workflow Studio or the Workflow Studio Connections list. The Outbound connections are listed in alphabetical order.

6. Navigate to or search for the OT Discovery Connections record.

7. You can view and edit connections by selecting **View Details**.
OT Discovery is the default connection.

8. On the OT Discovery connection page, select **Configure**.
The **Create Connection** window opens. To create a connection, select **Add Connection**.

9. In this window, fill in the following connection details as explained in the following table.

Connection details

Field	Description
Connection Name	Enter a unique name for the connection. The default connection has the name as OT Discovery and is read-only. For additional connections, enter a unique name for each. This field is mandatory.
Connection URL	Navigate to the Console and copy its URL and paste it into the Connection URL field. For example: https://OTDiscoveryConsole.net:8443/ This field is mandatory.
Use MID Server	Optionally, check this box to use a MID Server for the connection.
MID Server	Optionally, select a MID Server for the connection.
API Key	To get the API Key:

Field	Description
	a. Go to your Console and navigate to the Settings page. b. Open the API tab and select the Add  icon. c. In the Generate API Token window, select the expiration length you want and select Generate Token. d. The generated token is listed in the Active token list. e. Select the Copy icon to copy the token. f. Paste the token key into the API Key field. g. Select Save. This field is mandatory.

10. Navigate back to the **Configure the connection** page and select **Mark as complete**.

What to do next

The next step is to [Generate imports and validate the connections](#).

Generate imports and validate the connections

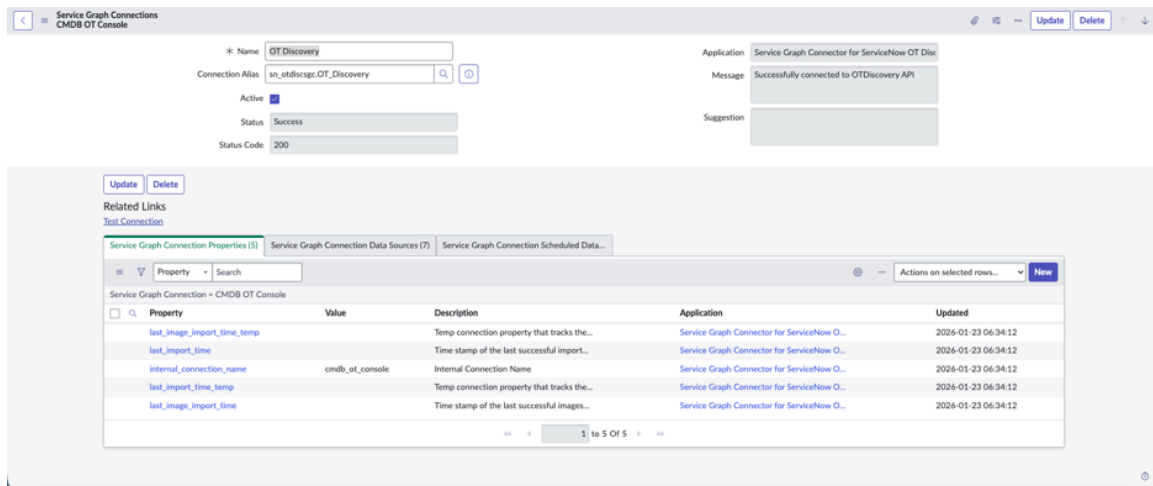
For each ServiceNow OT Discovery connection, configure the **name** and **run** as user for each import job. Each connection will generate a new **Scheduled Import Set** and **Data Source**.

Before you begin

Role required: admin

Procedure

- Next to the **Generate imports** task, select **Configure**.
The Generate imports for the OT Discovery Connection page opens.
- In the **Run As User** field, select System administrator.
This is the role within the platform who will run the schedules.
- Select **Generate**.
Because the Table permissions were set to Can Read, Can Create, and Can Update, this starts creating scheduled jobs in the background.
- When finished, the banner at the top of the page states "Successfully generated import objects for connection OT Discovery."
- Return to the Guided Setup and select **Mark as complete** next to the Generate imports task.
- For the **Validate the connection** section, select **Configure**.
- On the next page, check the box next to OT Discovery.
- Under the header, **Related Links**, select **Test Connection**
- Testing the connection takes a few moments and once completed, the page refreshes to show the test results.
The connection is successful if the Status Code is 200. If there's an Error Code and Error Message, the connection failed and further troubleshooting is required.



10. Select the OT Discovery link.

This opens the Service Graph Connector OT Discovery view.

11. The table lists the connection properties, the data sources that were generated and the 7 import schedules that were created.

12. This task tests:

- Is the Service Graph Connector able to reach the Instance.
- If so, is there a valid license on the Console.

If the connection was successful, but the Console license has expired, you may see a message in the Suggestion field asking you to reach out to your account representative.

13. Return to the Validate the connection section and select **Mark as complete**.

14. Return to the Guided Setup page.

Review and configure integration settings

To make the Service Graph Connector for ServiceNow OT Discovery simple to use, set options that let you modify the integration behavior to meet your business needs.

Before you begin

Be sure to complete all previous configurations for the Service Graph Connector for ServiceNow OT Discovery before beginning the following tasks.

Role required: admin

About this task

Configure the ServiceNow OT Discovery Classification Settings which define how ServiceNow OT Discovery categories are mapped to target CMDB classes. Configure additional settings based on Classification such as the CI naming strategy and if you permit OS classification. Default recommended classification settings are provided by the application which you can then configure for your needs.

Procedure

1. Select **Configure classification settings**.

- a. Next to the Configure classification settings task, select **Configure**.
- b. Review the default OT Discovery Classification Settings.

Note: The OT Discovery Classification Settings define how OT Discovery categories are mapped to the target ServiceNow Instance CMDB classes. It also defines how they are configured to additional settings based on classification, such as the configuration item (CI) naming strategy and whether to permit OS classification. The default recommended classification settings are provided by the application, which you can then configure for your needs.

- c. All the devices that are imported follow a default naming strategy.
- d. You have the flexibility at a class level to change the name.
- e. You can map the Target CMDB Class name to an OT Device type and can change the mapping settings.
- f. If any changes are needed, open the OT Discovery Classification Setting record and update the entries in the following fields.

OT Discovery Classification Setting fields

Field	Description
Active	If checked, the Classification Setting is used when classifying the devices. If unchecked, the Classification Setting is ignored.
Source Class	The class name of the source asset.
Network type	Defines whether this classification setting is for OT or IT devices only. Leave empty to include both types. If OT devices with a specific category must be classified into a separate class from IT devices, there are two definitions for the OT Discovery Category. One definition has the Network type set to OT with the classification for the OT devices. The other definition is set to IT for classifying the IT devices.
Target CMDB class	The CMDB class to target when importing the OT Discovery device.
OT device type	For OT devices, you can select the OT device type to apply the device type to the imported OT Discovery asset in the CMDB, if applicable.

2. Optional: Next, Configure system properties.

- a. Next to the Configure system properties task, select **Configure**.

Configure system properties

This record is in the **Service Graph Connector for ServiceNow OT Discovery** application, but **Global** is the current application. To edit this record click [here](#).

Properties

Service Graph Connector for ServiceNow OT Discovery Settings

(Optional) Comma-separated list of ServiceNow OT Discovery categories to filter the Asset import to. Default: blank

API Page Size: The maximum number of rows to be returned from a single REST call. Default: 500

500

API Max Timeout: The maximum amount of time to await a response when making REST calls to OTDiscovery. Default: 30000

30000

Load Raw API Data into Staging Table: When set to true, the raw API data for each row will be included in the staging tables along with the parsed data. This can be useful when trying to compare data imported data in ServiceNow vs what is available in the OTDiscovery API

☒ Yes ☐ No

Log Levels

Info

Save

Close

- b. The Configure System properties window opens.

- c. Review the System properties and adjust as needed for your instance configuration.

System properties

System property	Description
(Optional) Comma-separated list of OT Discovery categories to filter the Asset imports.	Filters the Asset import to only import assets of particular categories. For example, if you wanted to only import ICS Host and PLC category devices from the Discovery Console for OT, you could set this to PLC , I c s H o s t. Default: empty Note: These are categories defined on the Console side.
API Page Size	Maximum number of rows to be returned from a single REST call. (Optional) Default: 500
API Max Timeout	Maximum amount of time to wait for a response when making REST calls to OT Discovery. Default: 30000
Load Raw API Data into Staging Table	When set to true, the raw API data for each row is included in the staging tables along with the parsed data. This is useful when trying to compare data imported data into ServiceNow vs. what is available in the OT Discovery API.
Log Levels	Logging level verbosity to use for the application.

System property	Description
	(Optional) Default: Info

- d. Select **Save** and close the window.
- e. Return to the Configure system properties task and select **Mark as complete**.
- f. Return to the Guided Setup page.

What to do next

The next setup step is to [Set up scheduled import jobs](#).

Set up scheduled import jobs

Configure the scheduled import jobs.

Before you begin

Role required: admin

Procedure

1. In the Setup scheduled import jobs section select **Import sites**.
 - a. Next to the Import sites task, select **Configure**.
 - b. Select the Site Scheduled Data Import Job.
 - c. To manually execute the job, select **Execute Now**.
 - d. Return to the Guided Setup and select **Mark as complete** next to the Import sites task.
 - e. Next, in the Configure site mappings task, select **Configure**.
 - f. Review the list of imported sites.
 - g. Select the first site and in the form, fill in the following fields.
 - All field titles with * (asterick) next to them are mandatory and should be filled in.
 - Populate the **Site type** field. This field is mandatory. The value can be either OT or IT. If you select OT, all the hardware records imported later will also have OT device (cmdb_ot_entity) records related to them automatically. For any site with a Site type between IT and OT, set the **Site type** to **OT**.
 - Set the ISA assignment site. All the data in the site will import to the ISA assignment site you choose.
 - If applicable, populate the **Location** and **Company** fields.
 - Check the Active box.
 - Fill in the **Assigned Meta Data** section. Whatever you assign as Meta Data is copied onto all imported devices.

Note: Any value populated will be cascaded down to all CIs this Site is related to when the asset data is imported into the CMDB.
 - h. Select **Update**.
 - i. Return to the Guided Setup and select **Mark as complete**.
2. Do the **Configure scheduled jobs** task next.

By default, the ServiceNow OT Discovery scheduled jobs created during installation are inactive. All other jobs are configured to run after their parent job, the Site Scheduled Data Import Job. The only exception is the Asset Image import jobs, which run independently.

- a. Next to the Configure scheduled job task, select **Configure**.
- b. In the Scheduled Jobs list, open a site record.
- c. To activate the scheduled job, select the check box next to the **Active** field.
- d. In the **Run** and **Time** fields, select how often and when you want the job to run.

For example, daily at midnight.

- e. Select **Update**.
- f. Repeat these steps for each site in the Scheduled Jobs list.
- g. When you finish the sites, select the asset record from the Scheduled Jobs list.
- h. To activate the scheduled job, select the check box next to the **Active** field.

Note: You don't have to set the **Run** field for the asset record since the asset scheduled job automatically runs after the site scheduled job runs.

The following schedules jobs are available to import data:

- **Asset import:** This imports the OT Devices discovered into CMDB.
- **Network Zone import:** This imports the list of Managed Networks defined within the Site to support the deployment of OT Discovery.
- **Sensor import:** This imports list of all the Sensors used for OT Discovery deployment into the NIDS table.
- **Connection import:** This imports the list of communications between the devices.
- **Asset Images:** This imports the list of screenshots captured during the discovery process in the cmn_media table.

- i. Return to the Guided Setup and select **Mark as complete** next to the Configure scheduled job task.

3. Review imported data.

- a. Wait until the scheduled jobs are complete on their schedule or open the scheduled job and select **Execute Now** to execute it on demand.
- b. Once the jobs are complete, select **Configure** next to the Review imported data task.
- c. Review the imported CMDB data.
- d. Return to the Guided Setup and select **Mark as complete** next to the Review imported data task.

Result

You have completed the Service Graph Connector for ServiceNow OT Discovery Guided Setup. Review the [Use advanced configurations](#) section.

Use advanced configurations

Use the advanced configuration for the Service Graph Connector for ServiceNow OT Discovery to set up an asset extension points, a class calculator extension points, and a configuration item (CI) naming strategy extension points.

Before you begin

Role required: admin

Procedure

1. Optional: Set up an asset extension point.

Before being transformed by the Robust Transformer (RTE) and the Integration Hub ETL, the assets from the OT Discovery API are flattened into a standard format. If you want to include additional custom attributes into the flattened asset, you can choose to use the Asset Extension Point script. Once the extension point is implemented, you can transform and map the additional custom attributes using the Integration Hub ETL.

a. Navigate to **All > Service Graph Connectors > OT Discovery > Extension Points**

b. Select the **x_snc_mis_sec_sgc.SGMissionSecureAssetExtension** record.

c. In the Related Links section, select **Create implementation**

d. In the script, update the process function to include the desired additional attributes using JavaScript.

The following image is an example of a `custom_attribute` being added to the flattened asset.

The screenshot shows the 'Script Include' form for the `SGMissionSecureAssetExtension` class. The 'Name' field is `SGMissionSecureAssetExtension` and the 'API Name' is `x_snc_mis_sec_sgc.SGMissionSecureAssetExtension`. The 'Application' is 'Service Graph Connector for Mission Secure' and 'Accessible from' is 'This application scope only'. The 'Client callable', 'Mobile callable', and 'Sandbox enabled' checkboxes are unchecked. The 'Active' checkbox is checked. The 'Description' field contains: 'Implements extension point x_snc_mis_sec_sgc.SGMissionSecureAssetExtension. This extension allows users to have an intersection point between getting Asset from MissionSecure and inserting it into the staging table. Here you can modify or add additional properties'. The 'Script' field is expanded, showing the following JavaScript code:

```

1 var SGMissionSecureAssetExtension = Class.create();
2 SGMissionSecureAssetExtension.prototype = {
3   initialize: function() {
4   },
5   process: function(flattenedItem, apiItem) {
6     //Modify or add additional properties to the flattenedItem before returning flattenedItem which will
7     //be inserted into the staging table.
8     flattenedItem.custom_attribute = apiItem.extensions.customAttributes;
9     return flattenedItem;
10  },
11  type: 'SGMissionSecureAssetExtension'
12 };

```

e. Once the script is complete, validate the data by running a test load of the Data Source.

f. After you run the test load, navigate to **All > System Import Sets > SG-OT Discovery > Asset**.

g. Validate that the Data column contains the `custom_attribute` that you added in step 1d. If the custom attribute doesn't appear, compare the `api_data` to the data to correct the issue with your code.

h. Navigate to **Configuration > IntegrationHub ETL**.

i. Under CMDB Application SG-OT Discovery, select the **SG-OT Discovery Asset** record.

j. Under **1. Specify Basic Details**, select **Import Source Data and Provide Basic Details**.

k. Confirm that Integration Hub ETL is using a sample import with the **custom_attribute** from the previous step or scroll down and use the **Auto-pull a new import set** option.

l. Select **Save** and **Mark as Complete** to retrieve the import set.

Note: You may see error messages when navigating back to the ETL Transform Map Assistant. You can ignore these messages.

m. Use **Preview and Prepare Data** and select **CMDB Classes to Map Source Data** to transform and map the custom_attribute as desired.

2. Optional: Set up a class calculator extension point.

During transformation, classification of assets from the OT Discovery API is calculated based on the OT Discovery category and, optionally, the Network type of the Site (OT or IT) using the OT Discovery Classification Settings. An extension point is provided for additional advanced configuration which overrides the classification setting.

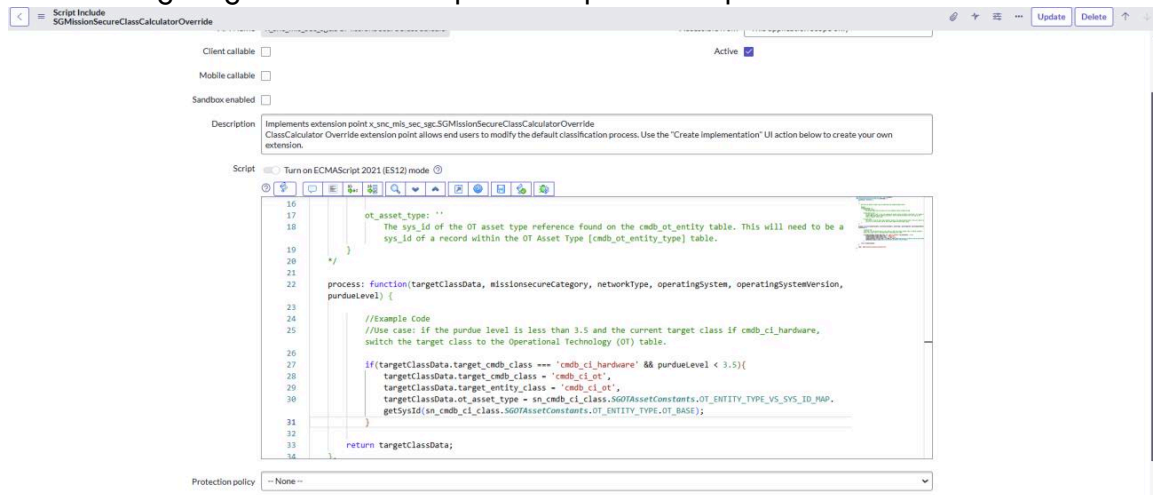
a. Navigate to **All > Service Graph Connectors > OT Discovery > Extension Points**.

b. Select the **x_snc_mis_sec_sgc.SGMissionSecureClassCalculatorOverride** record.

c. In the Related Links section, select **Create implementation**.

d. In the script, update the process function as desired.

The following image shows an example of an updated script.



3. Optional: Set up a configuration item (CI) Naming Strategy extension point.

The Service Graph Connector for OT Discovery comes with **JustNameFallbackIPAddressAndNetworkZone**, which is a default CI Naming Strategy. If you want to name the CIs differently, you can configure additional CI Naming Strategies using the extension point.

a. Navigate to **All > Service Graph Connectors > OT Discovery > Extension Points**

b. Select the **x_snc_mis_sec_sgc.SGMissionSecureCINameCalculation** record.

c. In the Related Links section, select **Create implementation**.

d. In the script include, update the following fields.

- Update the **Name** field to an appropriate name for the CI Naming Strategy.

You must start the name with **SGOTDiscoveryCINameCalculation** and add the rest of the name using camel-casing with no spaces or special characters. For example, **SGOTDiscoveryCINameCalculationAppendMAC**.

- In the **Script** field, update the `calculateCIName` function as needed.

e. Navigate to **Service Graph Connectors > OT Discovery > Classification Settings**.

f. Select the record that uses the new naming strategy.

g. Change the **CI naming strategy** field to the new CI Naming Strategy.

h. Repeat needed steps for any additional classification settings that should use your CI Naming Strategy.

Review additional Service Graph Connector for ServiceNow Operational Technology (OT) Discovery records

After completing the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup, review the unknown devices and log records.

Before you begin

Role required: admin

About this task

These are optional tasks.

Procedure

1. On your dashboard, navigate to **All > Service Graph Connector > ServiceNow OT Discovery**.
2. In the ServiceNow OT Discovery menu, you can review extended information about and settings for the Service Graph Connector for ServiceNow OT Discovery.
3. Scroll the topics under **ServiceNow OT Discovery** until you find **All Unknown OT Devices Missing Model & Manufacturer**.
This is a list of all the OT devices that were imported without a model number or name of their manufacturer.
4. Scroll the topics under **ServiceNow OT Discovery** until you find **All Unknown OT Devices Missing Model**.
This is a list of all the OT devices that were imported without a model number.
5. In the menu, scroll down to **App Logs**.
The App Log lists logs for all the OT Discovery applications within the Service Graph Connector scope. The columns are the creation date, the level, the log message, the App Scope, and the Source Script.
6. Now scroll to the **Last Imported Logs** entry in the menu.
The table lists a creation date, what the level of the message is, whether information or warning, and the source of the entry.
7. Use the items in the menu to review information from the Service Graph Connector for ServiceNow OT Discovery Guided Setup settings.

Support and troubleshooting

Common troubleshooting options when you set up the integration for the Service Graph Connector for ServiceNow OT Discovery.

Test the connection

You can test the connection after configuring your URL and credentials for the integration. If everything is configured correctly, the service graph connection displays a successful connection test without any error. If something goes wrong during the connection, the Service Graph connection displays the error message, error code, and response body from the API.

Service Graph Connections
Mission Secure

Name: Mission Secure

Connection Alias: x_snc_mis_sec_sgc.Mission_Se

Active: ☒

Status: Success

Status Code: 200

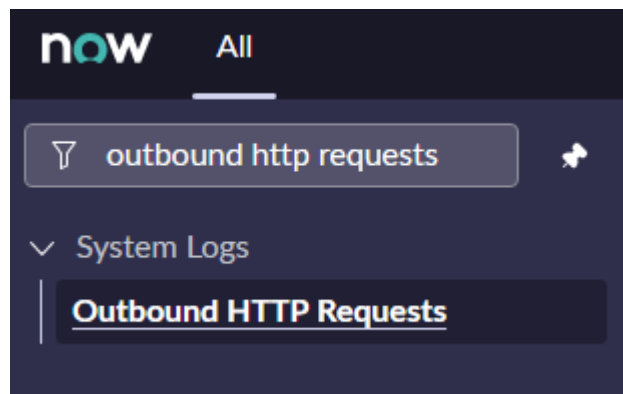
Application: Service Graph Connector for Missio

Message: Successfully queried Asset from the MissionSecure API

Suggestion:

Review Outbound HTTP Request records

You can also review the Outbound HTTP Request records associated with the test. Navigate to **All > System Logs > Outbound HTTP Requests**.



In the list view, you should see the URL hostname that you specified when setting up the connection parameters. Open this record to view the connection details.

Outbound HTTP Log
Created 2025-02-11 07:36:31

HTTP method: GET

Response status: 200

Created: 2025-02-11 07:36:31

Response time (ms): 1,565

URL: https://cmdblab.missionsecure.net:8443/api/externalapitoken?page=1&pagesize=500

Log Level: Source Request Response

The configured log level determines which values are logged. Some values are logged only if the log level is Elevated or All. [More info](#)

Log level: All

By default, the log level is set to Basic, so you can't see the response body or quest body, but the response status indicates the issue. For example, a 401 in the Response status indicates an unauthorized request. To resolve the issue, navigate to the connection and verify that you have

the correct Client ID and Client Secret entered for the connection. For more information, see [Install the Service Graph Connector for ServiceNow Operational Technology Discovery](#).

Additional diagnosis

If you must diagnose further, you can override the log level to give more information, for example using the global system properties. Navigate to the system properties by going to **sys_properties.list** in the application navigator and update the **glide.outbound_http_log.override** to the value true and update the **glide.outbound_http_log.override.level** to an appropriate value. For example, change value to **All**.

Note: You can perform action only for a limited period of time for troubleshooting. Make sure you revert the changes to the original configuration.

Name	Value	Type	Application	Description	Updated	Updated by
*glide.outbound_http_log.override	Search	Search	Search	Search	Search	Search
glide.outbound_http_log.override	true	true false	Global		2023-10-12 10:14:49	Jessica.hanrahan
glide.outbound_http_log.override.level	all	string	Global		2023-10-12 10:13:48	Jessica.hanrahan

With extended logging turned on, you can provide additional details for requests after that to give more context to the issue.

If you encounter a response status of 401, it's typically an issue with your credentials. To resolve, navigate to the connection in the Flow Designer and verify that the API Key is filled in as expected with the correct value.

If you encounter any issues with the flattening of the Asset or missing data from the API, you can run a test load and validate the flattened data from the Staging table. Then compare it with the **api_data** to see if the data was provided from the API.

SGC Central

Use SGC Central to set up your Service Graph Connector for ServiceNow OT Discovery, then import data from your OT Discovery environment into your ServiceNow instance.

SGC Central is recommended for setting up the Service Graph Connector for ServiceNow OT Discovery. It simplifies connector deployment with intuitive setup options and step-by-step playbook guidance. Alternatively, you can use the original Guided Setup. See [Service Graph Connector for ServiceNow OT Discovery Guided Setup](#).

SGC Central is available as a view in the CMDB Workspace or can be searched for in the **All** menu. The application enables you to discover and install Service Graph Connectors, and then effectively manage the full life cycle of creating, editing, monitoring, and debugging connections. The SGC Central application also verifies that connectors remain supported and up-to-date with certified partners.

Use the links in the Related Topics section to learn more about SGC Central.

SGC Central prerequisites

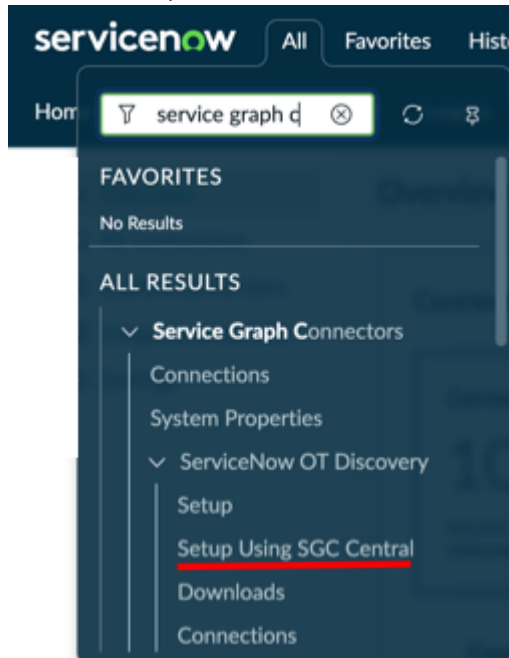
Get started with SGC Central and set up the prerequisites for the Service Graph Connector for ServiceNow OT Discovery

Before you begin

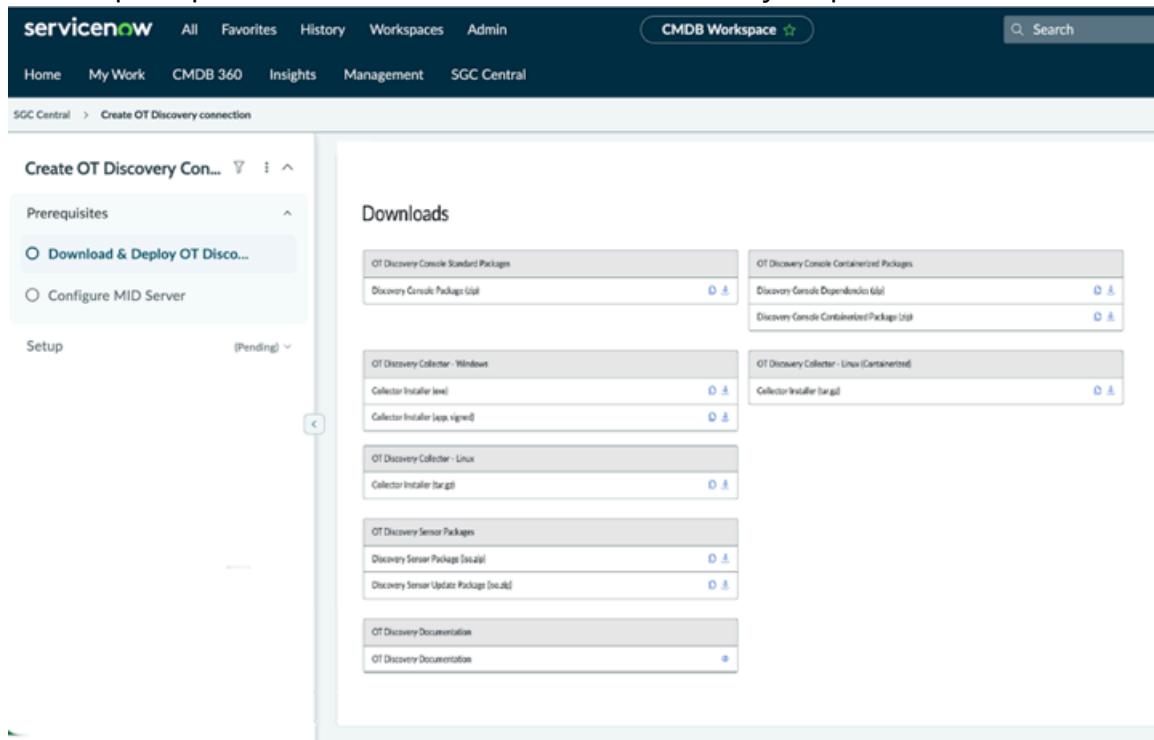
Role required: admin

Procedure

1. Navigate to the **All** menu and type in search field **service graph connector**.
You can also access SGC Central by navigating to the CMDB Workspace.
2. In the results, under ServiceNow OT Discovery, the **Setup Using SGC Central** option displays.



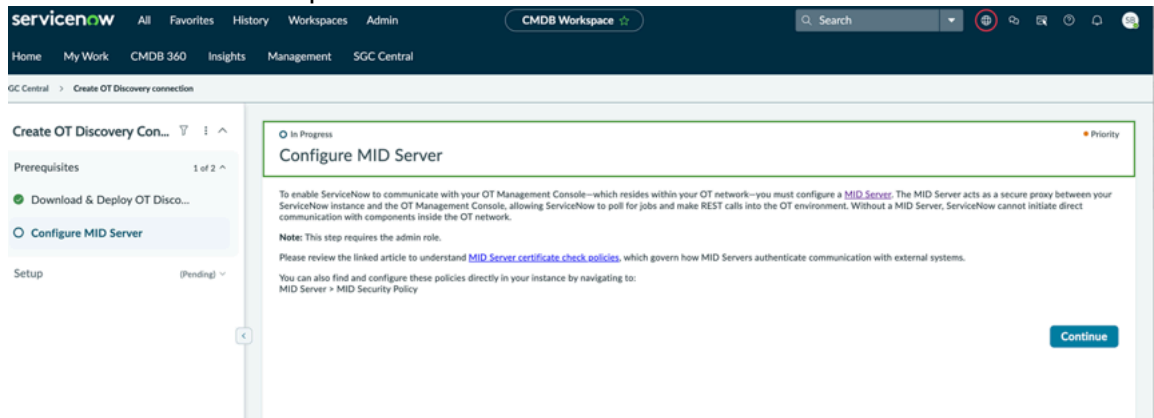
3. Select the **SGC Central** tab.
4. There are two prerequisites you much complete before you can create connections for the Service Graph Connector for ServiceNow OT Discovery:
5. The first prerequisite is download and install the OT Discovery components.



- a. Download and install the Discovery Console for OT package.
- b. Download and install the Discovery Sensor for OT package (ISO and OVR).
- c. Download and install the OT Discovery Collector package that's compatible with your OS.

Note: You can download and install the Console and Collector containerized packages. Be sure to select the Collector package that is compatible to your OS. For more information, see [Air-gapped networks and OT Discovery installation](#).

6. The second prerequisite is to configure the MID Server. Configure the MID Server using the MID Server Guided Setup. Select the link to review the MID Server certificate check policies.



7. Verify that the prerequisites are complete and select **Continue**.

Configure and test connections

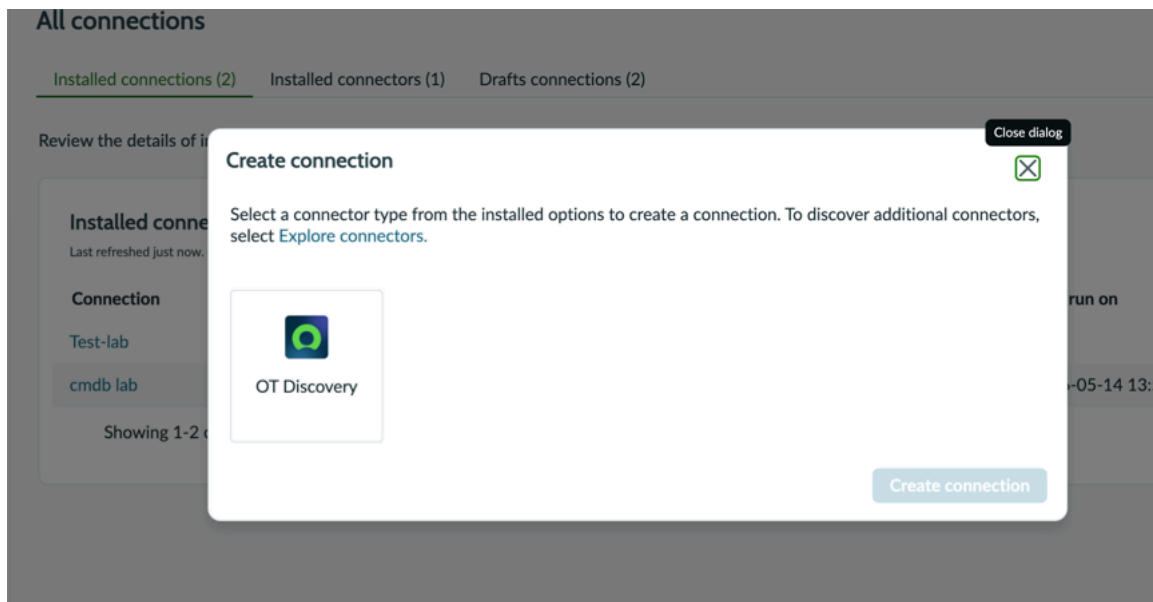
The SGC Central playbook launches when you start to configure and test connection.

Before you begin

Role required: admin

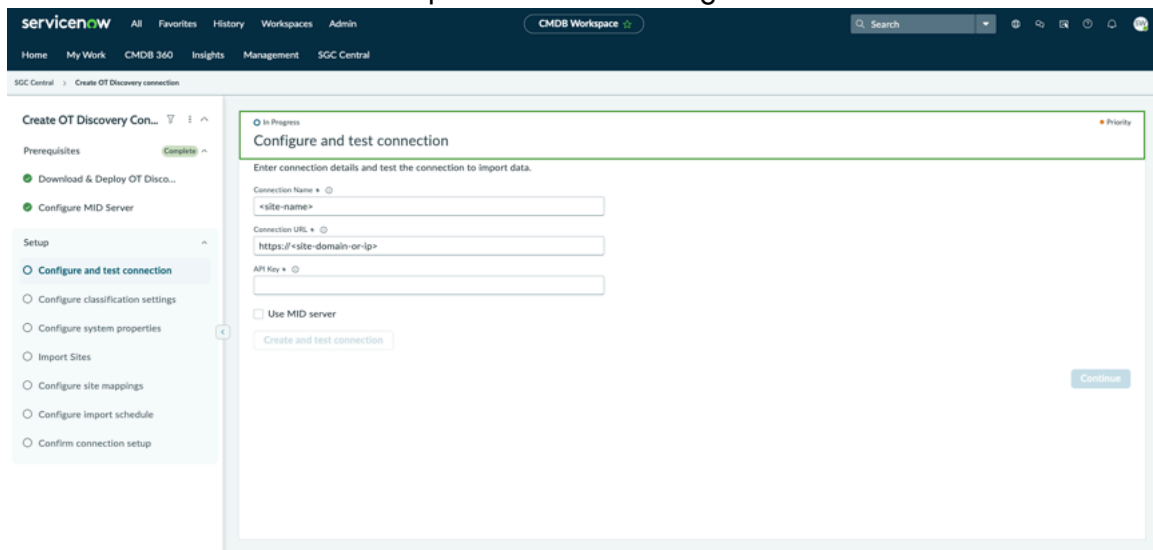
Procedure

1. From the **Setup** section, select **Configure and test connections**. After you select the **Create connection** button, a guided playbook experience launches automatically. The playbook walks you through each required configuration step for the Operational Technology Discovery connector.
2. Select the **Create connection** button.



The **Create connection** window opens.

3. In the **Create connection** window, select **OT Discovery**.
4. Select the **Create connection** button in this window.
5. Fill in the connection details as explained in the following table.



Connection details

Field	Description
Connection Name	Enter a unique name for the connection. The default connection has the name as OT Discovery and is read-only. For additional connections, enter a unique name for each. This field is mandatory.
Connection URL	Navigate to the Discovery Console for OT and copy its URL and paste it into the Connection URL field.

Field	Description
	For example: https://OTDiscoveryConsole.net:8443/ This field is mandatory.
API Key	To get the API Key: - Go to your Console and navigate to the Settings page. - Open the API tab and select the Add  icon. - In the Generate API Token window, select the expiration length you want and select Generate Token. - The generated token is listed in the Active token list. - Select the Copy icon to copy the token. - Paste the token key into the API Key field. - Select Save. This field is mandatory.
Use MID Server	This is optional. Check this box to use a MID Server for the connection.

6. Select the **Create and test connection** button.
7. If successful, you see the **Connections verified** banner.
8. Select **Continue** to move to the next step.

Configure classification settings in SGC Central

In SGC Central, you can configure the Service Graph Connector for ServiceNow OT Discovery classifications settings to define how OT Discovery categories are mapped to the CMDB classes.

Before you begin

Role required: admin

Procedure

1. When you select Continue in the Configure and test connections step, the Configure classification settings step opens.
2. Review the classification settings.

Note: The OT Discovery classification settings define how OT Discovery categories are mapped to the target ServiceNow Instance CMDB classes. It also defines how they are configured to additional settings based on classification, such as the configuration item (CI) naming strategy and whether to permit OS classification. The default recommended classification settings are provided by the application, which you can then configure for your needs.

3. In this step, you can edit, export, or create settings.
You can select **Skip** to skip this step.
4. All the devices that are imported follow a default naming strategy.
5. You have the flexibility at a class level to change the name.
6. You can map the Target CMDG Class name to an OT Device type and can change the mapping settings.
7. If any changes are needed, select the OT Device Type, open the classification settings record, and update the entries in the following fields:

OT Discovery Classification Setting fields

Field	Description
Active	True. If checked, the Classification Setting is used when classifying the devices. If unchecked, the Classification Setting is ignored.
Source Class	The class name of the source asset.
Network type	Defines whether this classification setting is for OT or IT devices only. Leave empty to include both types. If OT devices with a specific category must be classified into a separate class from IT devices, there are two definitions for the OT Discovery Category. One definition has the Network type set to OT with the classification for the OT devices. The other definition is set to IT for classifying the IT devices.
Target CMDB class	The CMDB class to target when importing the OT Discovery device.
OT device type	For OT devices, you can select the OT device type to apply the device type to the

Field	Description
	imported OT Discovery devices in the CMDB, if applicable.

8. Select **Continue** to move to the next step.

Configure system properties on SGC Central

In this step, review and modify the configurable system properties included with the integration.

Before you begin

Role required: admin

Procedure

Next, review and modify **Configure system properties** included in the integration.

a. Next to the Configure system properties task, select **Configure**.

b. The Configure System properties window opens.

c. Review the System properties and adjust as needed for your instance configuration.

System properties

System property	Description
(Optional) Comma-separated list of OT Discovery categories to filter the Asset imports.	Filters the Asset import to only import assets of particular categories. For example, if you wanted to only import ICS Host and PLC category devices from the Discovery Console for OT, you could set this to <code>PLC , IcsHost</code>. Default: empty Note: These are categories defined on the Console side.

System property	Description
API Page Size	Maximum number of rows to be returned from a single REST call. Default: 500
API Max Timeout	Maximum amount of time to wait for a response when making REST calls to OT Discovery. Default: 30000
Load Raw API Data into Staging Table	When set to true, the raw API data for each row is included in the staging tables along with the parsed data. This is useful when trying to compare data imported data into ServiceNow vs. What is available in the OT Discovery API.
Log Levels	Logging level verbosity to use for the application. Default: Info

d. Select **Save** and move to the next step.

Import Sites

In SGC Central the next step is to import the Sites.

Before you begin

Role required: admin

Procedure

1. In the SGC Central setup process, you must import sites before importing assets.

In Progress

Priority

Import Sites

Before importing assets from ServiceNow OT Discovery, we need to first import the Site data into the ServiceNow OT Discovery Site Mapping table in ServiceNow.

1. Open the Site Scheduled Data Import Job.
2. Manually execute import job by clicking the Execute Now Button.

Note:

- In this step, only execute the Import Site Scheduled Data Import. Activation of the scheduled data import is not required at this stage.
- In the subsequent step, "Configure Import Schedule" ensure that the scheduled data import is activated.

Import schedules 1

Last refreshed just now.

Scheduled Data Import	Parent	Run	Data source	Active	Updated
[Test-lab] Site	(empty)	Daily	[Test-lab] Site	false	2026-05-19 07:05:17

Showing 1-1 of 1

1

50 rows per page

Continue

2. Open the **Site Scheduled Data Import** job; that is, select the site displayed under **Scheduled Data Import**.
3. The Configure import schedule window opens for that site.

Configure import schedule

Run this import schedule now to start bring in data at the earliest. **Execute Now**

Set up import schedule.

Name: [Test-lab] Site

Application: Service Graph Connector for ServiceNow O...

Data source: [Test-lab] Site

Run as:

Save

4. Select the **Execute Now** button to manually import.

Execute import schedule

You are about to execute the import schedule '[Test-lab] Site'. The import may take a few hours but will run in the background, enabling you to continue working.

Cancel **Execute Now**

5. Repeat these steps for additional sites.
6. Select **Continue** to move to the next step.

Configure site mappings

Importing the site data must be complete before you can move onto configure site mappings.

About this task

Before proceeding, review and configure imported ServiceNow OT Discovery site mapping records and verify that the site data has been fully imported via the site scheduled data import. The site mapping records will not be available until the import is complete.

Before you begin

Role required: admin

Procedure

1. In the **Configure site mappings** task, scroll down to review the list of imported sites.

SGC Central > Create OT Discovery connection

Create OT Discovery Con... ▾ ⓘ ⌵

Prerequisites Complete ▾

Setup 3 of 7 ^

- ☐ Configure and test connection
- ☒ Configure classification settings
- ☒ Configure system properties
- ☒ Import Sites
- ☒ **Configure site mappings**
- ☐ Configure import schedule
- ☐ Confirm connection setup

Configure site mappings 4 Last refreshed just now.

Configure site mappings

In Progress Priority

Before proceeding with review and configure imported ServiceNow OT discovery site mapping records, ensure that the site data has been fully imported via the site scheduled data import. The site mapping records will not be available until the import is complete.

How to Check Site Data Import Progress:

1. From the ServiceNow OT Discovery application menu, click the **Import Schedules** menu item. This will display all scheduled data imports.
2. Open the most recently executed scheduled data import for the site.
3. On the scheduled data import record, scroll to the **Related Lists** section and open the **Executions** related list.
4. Open the latest execution record to view the progress of the site data import.
5. Wait until the execution status shows the import is complete.
6. Once the site data has been imported, return to the Configure Site Mappings step and click the **Refresh** button to load the newly imported site records.

Note: OT Device (cmdb_ot_entity) records will only be created if the Site type is set to OT.

1. Review Site and manually populate the Equipment model entity(Mandatory), and Site type (Mandatory). Additionally, you may populate the Location, Company, and Assigned Meta Data section where applicable.

Note: Any value populated will be cascaded down to all CIs this Site may be related to when the Asset data is imported into the CMDB.

2. Set the Site type value to either OT or IT. If OT is selected, all hardware records imported later will also have OT Asset (cmdb_ot_entity) records related to them automatically. For any Site with a Site type which is mixed between IT and OT, please set to 'OT'.

Refresh Reset Filter Edit Export New

2. Select the first site and in the form that opens, fill in the fields as follows.

Configure site mappings Close dialog

ServiceNow OT Discovery Site ID *

ServiceNow OT Discovery Site Name *

Site type * OT ▾

ISA assignment site *

Location

Company

☒ **Active**

Owned by

Approval group

Managed by

Managed by group

Supported by

Support group

- a. All field titles with * (asterick) next to them are mandatory and should be filled in.
- b. Select a value in the **Site type** field.
The value can be either **OT** or **IT**. If you select **OT**, all hardware records imported later also have OT device (*cmdb_ot_entity*) records related to them automatically. For any site with a site type between IT and OT, select **OT**.
- c. Select an **ISA assignment site**.

All data in the site imports to the ISA assignment site you select.

d. If applicable, populate the **Location** and **Company** fields.

e. Check the **Active** box.

Note: Any value populated is cascaded down to all configuration items (CIs) this Site is related to when the asset data is imported into the CMDB.

3. Select **Continue** to move to the next step.

Create import schedule

After importing sites and configuring site mappings, you can create an import schedule.

Before you begin

Role required: admin

Procedure

1. Do the **Configure scheduled jobs** task next.

By default, the ServiceNow OT Discovery scheduled jobs created during installation are inactive. All other jobs are configured to run after their parent job, the Site Scheduled Data Import Job. The only exception is the Asset Image import jobs, which run independently.

The following schedules jobs are available to import data:

- **Asset import:** This imports the OT Devices discovered into CMDB.
- **Network Zone import:** This imports the list of Managed Networks defined within the Site to support the deployment of OT Discovery.
- **Sensor import:** This imports list of all the Sensors used for OT Discovery deployment into the NIDS table.
- **Connection import:** This imports the list of communications between the devices.
- **Asset Images:** This imports the list of screenshots captured during the discovery process in the cmn_media table.

2. When done, select **Mark as complete**.

The screenshot shows the 'Create OT Discovery connection' page in ServiceNow. On the left, a sidebar lists prerequisites and setup steps. The 'Import schedules' table is displayed with columns: Scheduled Data Import, Parent, Run, Data source, Active, and Updated. The table shows a hierarchy of jobs, with 'Parent: [Test-lab] Site (5)' expanded to show five child jobs: Network Zone, Asset, Software, Sensor, and Connection. All jobs are currently inactive (false) and were last updated on 2026-05-19 07:05:18.

Scheduled Data Import	Parent	Run	Data source	Active	Updated
Parent: (empty) (2) Show all					
[Test-lab] Asset Image	(empty)	Daily	[Test-lab] Asset Image	false	2026-05-19 07:05:18
[Test-lab] Site	(empty)	Daily	[Test-lab] Site	false	2026-05-19 07:05:17
Parent: [Test-lab] Site (5) Show all					
[Test-lab] Network Zone	[Test-lab] Site	After Parent Runs	[Test-lab] Network Zone	false	2026-05-19 07:05:18
[Test-lab] Asset	[Test-lab] Site	After Parent Runs	[Test-lab] Asset	false	2026-05-19 07:05:18
[Test-lab] Software	[Test-lab] Site	After Parent Runs	[Test-lab] Software	false	2026-05-19 07:05:18
[Test-lab] Sensor	[Test-lab] Site	After Parent Runs	[Test-lab] Sensor	false	2026-05-19 07:05:18
[Test-lab] Connection	[Test-lab] Site	After Parent Runs	[Test-lab] Connection	false	2026-05-19 07:05:18

Showing 1-2 of 2

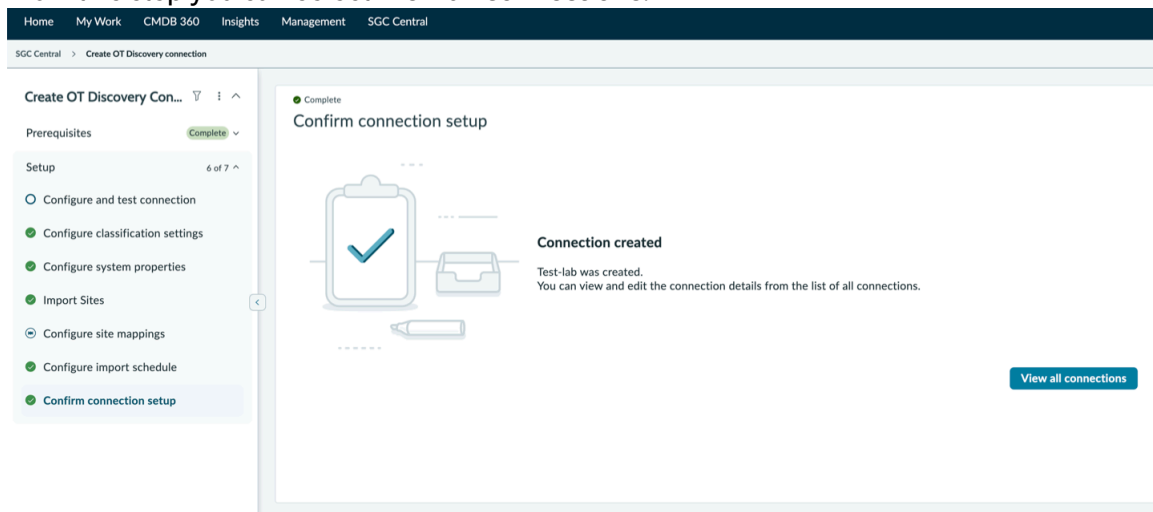
50 rows per group

Continue

3. Navigate to **Confirm connection setup**.

4. Check the connection setup to confirm it is valid.

5. From this step you can select **View all connections**.



Review imports

This section reviews all your importation settings in SGC Central.

About this task

After you have completed the steps of the SGC Central OT Discovery playbook, you can review your imports by following this process.

Before you begin

Role required: admin

Procedure

1. Navigate to the **All** menu and type in "discovery" in the search field.

2. From the drop-down list, choose a review task.

After completing the configurations and scheduling imports in the SGC Central, you can now go back and review the settings. Select:

- Review Imported OT Devices
- Review Imported Network Connections
- Review Imported Images

3. For example, select **Review Imported Images**.

The window displays:

Name	Accepted by	Acquisition Date	Default	Description	Image	Media Type	Record ID	Record Title	Sequence
Screenshot	Imported	Imported	True	15x10x10x 1000 1000 1000 1000		Image	PIC: 17 16 16 100 100 100 100	PIC: 17 16 16 100 100 100 100	
Screenshot	Imported	Imported	True	10x10x10x 1000 1000 1000 1000		Image	PIC: 17 16 16 100 100 100 100	PIC: 17 16 16 100 100 100 100	
Screenshot	Imported	Imported	True	10x10x10x 1000 1000 1000 1000		Image	PIC: 17 16 16 100 100 100 100	PIC: 17 16 16 100 100 100 100	
Screenshot	Imported	Imported	True	10x10x10x 1000 1000 1000 1000		Image	PIC: 17 16 16 100 100 100 100	PIC: 17 16 16 100 100 100 100	

4. Select **Review Imported OT Devices**.

The window displays:

OT Devices View: All OT Devices OT device Search									
All > OT device Class > OT Control Module > OT device Discovery source > 5G-OTDiscovery									
☐	OT device	OT display name	OT device type	Class	Manufacturer	Model number	Firmware version	Description	Purdue level
	172.16.254.152 @ DEFAULT	172.16.254.152 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.184 @ DEFAULT	172.16.254.184 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.100 @ DEFAULT	172.16.254.100 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.158 @ DEFAULT	172.16.254.158 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.179 @ DEFAULT	172.16.254.179 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.118 @ DEFAULT	172.16.254.118 @ DEFAULT	(empty)	Hardware	(empty)				
	02uscanapd0000.caona.missionsecure.net	Lab Support Equipment	(empty)	Hardware	(empty)				
	172.16.254.159 @ DEFAULT	172.16.254.159 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.17.200 @ DEFAULT	HMI	(empty)	Linux Server	OtherIoT				
	172.16.27.102 @ DEFAULT	172.16.27.102 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.20.125 @ DEFAULT	172.16.20.125 @ DEFAULT	(empty)	Hardware	(empty)				
☒	172.16.254.174 @ DEFAULT	172.16.254.174 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.123 @ DEFAULT	172.16.254.123 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.147 @ DEFAULT	172.16.254.147 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.141 @ DEFAULT	172.16.254.141 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.164 @ DEFAULT	172.16.254.164 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.169 @ DEFAULT	172.16.254.169 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.254.178 @ DEFAULT	172.16.254.178 @ DEFAULT	(empty)	Hardware	(empty)				
	172.16.18.201 @ DEFAULT	172.16.18.201 @ DEFAULT	PLC	PLC	Econolite				
	172.16.250.100 @ DEFAULT	172.16.250.100 @ DEFAULT	PLC	PLC	AllenBradley				

Feedback on OT Discovery

To provide feedback on OT Discovery you can submit a NOW idea on ServiceNow support.

Now idea

- To open a NOW idea, log in to the support portal. When filling out the form, set the "Title" field to "Feedback on OT Discovery" and set the Product field to "Operational Technology Manager".
- When sharing data related to unknown devices (that is, devices that were not accurately identified/classified), provide additional information related to manufacturer, brand, product model, and version.
- DO NOT share any sensitive or confidential information, including proprietary information or data specific to a customer or user, such as IP addresses, user information, or passwords when submitting this form.

Note: To find the **Feedback on OT Discovery** page, enter "OT Discovery" in the **All** menu in your instance or navigate directly to the Create an Idea form: https://support.servicenow.com/now?id=create_edit_idea&sysparm_module_id=enhancement_requests.

IT Discovery for Operational Technology (OT) Networks

You can use the IT Discovery for Operational Technology (OT) Networks function to discover IT class OT devices. These devices are located in designated Purdue levels within 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 IT Discovery for OT Networks process operates in a manner that is similar to the standard Discovery processes.