USER GUIDE

ADMIN CONSOLE

Product	Snow Inventory
Version	5.2
Release date	2017-09-20
Document date	2018-01-03

CONTENTS

1 INTRODUCTION

This document describes administration and configuration of Snow Inventory 5 Servers and Agents using the Snow Inventory Admin Console.

The graphical user interface that is used for management of Snow Inventory 5 and the Snow Inventory Agents is called the Snow Inventory Admin Console. It is accessed via Snow Management and Configuration Center, which can be installed on any Snow Inventory server as well as on any workstation used by the IT administrators.

The Admin Console gives the administrator an overview of the environment including system performance, and status of the agents and the inventory data. Since the agents include their latest log when sending the inventory results to the server, detailed information on agent status and history is available for all platforms.

Information on agent versions and configurations is also available in the Admin Console. The administrator gets an overview of all the different Inventory Agent configurations and has the possibility to edit existing configurations, and create new ones. Also, the administrator can trigger a remote scan of Windows devices from the Admin Console.

1.1 UPDATE PROCEDURES

Any changes to the Inventory Agent, for example agent updates, new configurations, or requests of immediate scans, will be sent to the agent at the next scheduled communication time with the server. For the Inventory Agents for Linux, Unix, and macOS that normally means the next scheduled scan, while for the Windows agent it means the next reoccurring handshake which by default occurs every 5 minutes.

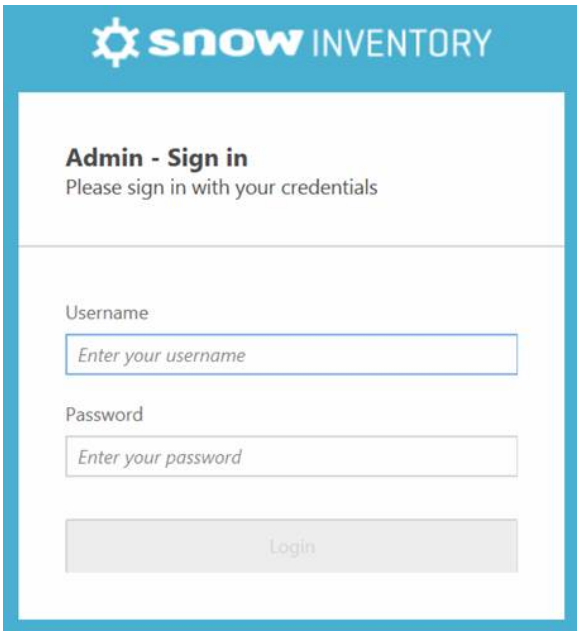
2 GENERIC INFORMATION

For best user experience when using the Snow Inventory Admin Console, a minimum screen resolution of 1280 x 800 is recommended.

2.1 LOGIN

The Snow Inventory Admin Console is accessed via the Snow Management and Configuration Center.

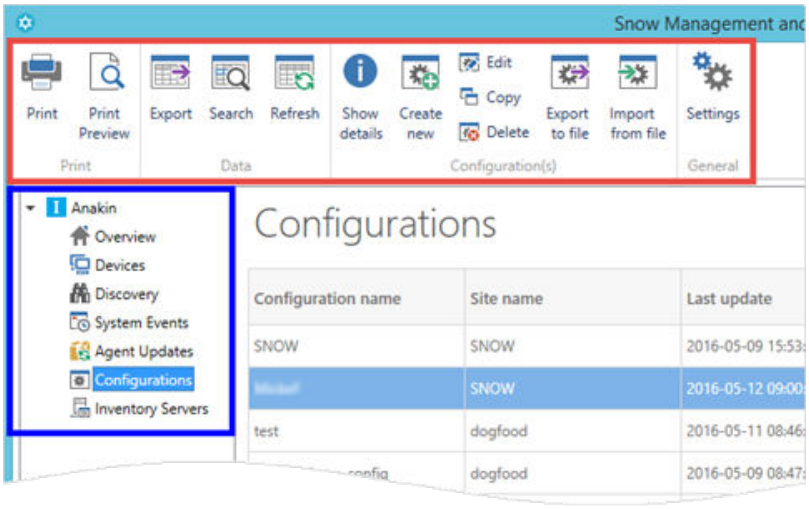
1. In the **Username** and **Password** boxes, type credentials of a Snow user with permissions to logon to the Snow Inventory Server.
2. Click **Login**.



2.2 MAIN MENUS

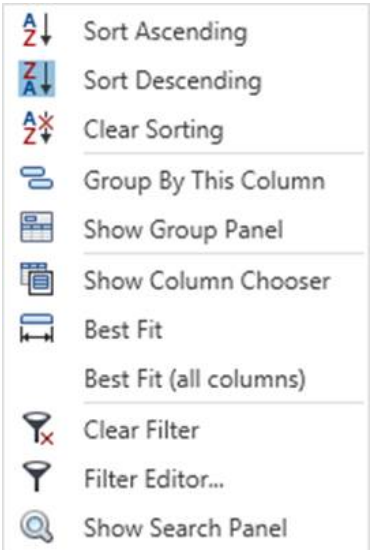
There are two main menus in Snow Inventory Admin Console:

- **Command** (marked in red)
  Available tasks for a selected category view
- **Category** (marked in blue)
  Available categories and related views



2.3 VIEWS

The available views in the Admin Console can be sorted, grouped, and filtered. Searches can be made, and columns can be added to or removed from the views.



2.3.1 SORT

To sort the view by a column, click that column header. To reverse the sorting order, click the same column header once again.

As an alternative, right-click the column header and select **Sort Ascending** or **Sort Descending**. Select **Clear Sorting** to restore the view to its original appearance.

2.3.2 GROUP

To group the view by a certain column, right-click that column and select **Group by this Column**.

As an alternative, right-click the column header and select **Show Group Panel**. Drag the selected column header to the panel to group by that column. The view can be grouped in several levels. Ungroup by dragging the column(s) back to the header in the **Group Panel** view

2.3.3 COLUMN CHOOSER

To customize the layout of a current view, right-click the column header and select **Show Column Chooser**. Use drag-and-drop when moving the columns between the view and the **Column Chooser** window.

2.3.4 FILTER

Click the **Filter editor** icon in the column header to see available information to filter on. For advanced filtering with several criteria, right-click the column and select **Filter Editor**.

2.3.5 SEARCH

To make a search, right-click the column header and select **Show Search Panel**. Matches are displayed as search criteria are typed in the box.

To hide the search box, click **Close** or right-click the column header and select **Hide Search Panel**.

2.4 REMOTE ADMINISTRATION

Snow Management and Configuration Center (SnowMACC) does not have to be run on the same server where Snow Inventory Server or Snow License Manager is installed. The files can easily be copied to any other server, desktop, or laptop on the network.

In this scenario Snow Inventory Server and Snow License Manager are installed on a server called **Server A**. The computer that will run SnowMACC with the plugins for Snow Inventory and Snow License Manager is called **Computer B**.

1. Copy the folder **Snow Management and Configuration Center** from **Server A** to **Computer B**.
2. On **Computer B** and in the **Snow Management and Configuration Center** folder, create a sub-folder called **PlugIns**.
3. On **Computer B** and in the **PlugIns** folder, create two sub-folders: one called **Inventory** and one called **SnowLicenseManager**.
4. On **Server A**, copy all the files in the **Snow Inventory\InventorySMACCPlugin** folder to the created **PlugIns\Inventory** folder on **Computer B**.
5. On **Server A**, copy all the files in the **Snow License Manager\Tools\SmaccPlugin** folder to the created **PlugIns\SnowLicenseManager** folder on **Computer B**.
6. Start SnowMACC.
   The two plugins are available for usage.

NOTE
Copied plugins will not be updated by the Snow Update Service (SUS). To update them manually, repeat the procedure described above.

3 CATEGORY VIEWS

This chapter describes the category views of the Admin Console and the available commands of each view.

3.1 OVERVIEW

On the **Overview** page the number of inventoried devices over the last 30 days are presented in two graphs; one aggregated (cumulative) graph and one per-day graph. Also, summaries of the information available in the **Devices**, **Agent updates**, and **Configurations** views are presented.

Section	Description
Device inventory status	Shows information on when the devices last reported data to the server. The information is shown both as a pie chart and as a list.
Agent with latest version	Shows the latest, available version of the agent for each platform, and also information on (in percentage) how many out of the total number of agents that have that version. Point to the bar to see additional information.
Configurations	Shows a summary of the **Configurations** view. The **Published** configurations reflects the number of configurations that have been created and deployed via the Admin Console compared to the **Total** number of inventoried configurations.
Latest agent version	Shows information on any new versions of the agents.

3.2 DEVICES

On the **Devices** page information on discovered and inventoried computers and other devices are presented in views. A number of views are delivered with the installation, and new can be created to support customer needs. Also, filters can be added to the views to refine them even further.

The inventoried devices are identified using the following properties:

- sitename
- hostname
- biosserialnumber
- uniqueidentifier (i.e. SID on Windows machines)

In case no scan result has yet been processed for a device, the name of the device is shown in light-gray italics in the **Device name** column, and all other columns are empty. This can happen in the following scenarios:

- **The server is aware of the device, but no inventory has yet been performed**
  When the Inventory agent is installed, it initially performs a "heartbeat" with the server on a regular basis (this is configurable using the **http.poll_interval** setting). The heartbeat does not contain a scan result, so until the first scan is scheduled and received, the computer name will be shown in light-gray italics.

- **The maximum unit count granted by the license has been reached**
  When the license capacity has been reached, no additional inventory results will be processed and the names of the overage computers will be shown in light-gray italics.
- **The inventory result is corrupt**
  This is a very rare scenario but can theoretically happen.

Devices cannot be automatically deleted in Inventory. To delete a device in Inventory, either delete it manually in the Admin Console, or use functionality in Snow License Manager.

3.2.1 COMMANDS

The following commands are available on the **Devices** page:

Command	Description
Export	Export the information as it is displayed on the **Devices** page to file. Any grouping or sorting will apply.
Search	Show (or hide) the search box
Refresh	Refresh the content of the view
Add view	Create a new custom view
Edit view	Edit a selected custom view
Copy view	Create a new custom view by copying an existing view
Delete view	Delete a selected custom view
Show details	Show details of a selected device
Initiate scan	Run a scan of a selected device. For more information, see Update procedures.
Delete	Delete data associated with the selected device(s). Note that data for any deleted device will reappear the next time the device reports.

3.2.1.1 DEVICE DETAILS

To see details of a specific device, double-click the device, or select the device in the list and then click **Show details**.

A summary is displayed in the main window. A container for the device is added under **Devices** in the category structure with the following sub-containers:

- System
- Network
- Hardware
- Software
- Oracle
- Peripherals
- Users

- Custom
- Log file
- Virtualization

Click to expand each sub-container and have the details presented in the main window.

3.3 DISCOVERY

On the **Discovery** page information on discovered computers and other devices are presented in views. These computers/devices do not have an Inventory agent installed. A number of views are delivered with the installation, and new can be created to support customer needs. Also, filters can be added to the views to refine them even more.

The discovered devices are identified using the following properties:

- hostname
- IP address
- MAC address

The **Discovery** page can be used for deployment of the Inventory Agent (Windows only). For more information, see Deploy an agent.

A discovered device cannot be automatically deleted in Inventory. It will remain visible on the Discovery page until either an Inventory agent has been deployed to it, or it is manually deleted in the Admin Console.

3.3.1 COMMANDS

The following commands are available on the **Discovery** page:

Command	Description
Export	Export the information as it is displayed on the **Discovery** page to file. Any grouping or sorting will apply.
Search	Show (or hide) the search box
Refresh	Refresh the content of the view
Add view	Create a new custom view
Edit view	Edit a selected custom view
Copy view	Create a new custom view by copying an existing view
Delete view	Delete a selected custom view
Create deployment	Deploy a package to a selected discovery (Windows only)
Delete	Delete a discovery entry

3.3.1.1 DISCOVERY DETAILS

To see details of a specific discovery, click the discovery in the list. Information such as **Source**, **Name**, **Network**, and **Active Directory** is shown on the bar to the right of the main window.

3.3.2 DISCOVERY METHODS

Computers and devices can be discovered using LDAP lookups in an Active Directory, or by using the following technologies for network discovery on specific IP address ranges:

- SNMP (SNMPv1)
- SSH
- WinRPC/WMI
- ICMP ("ping")
- TCP/IP fingerprinting
- DNS lookup
- NIC manufacturer lookup.

When TCP/IP fingerprinting is enabled, discovery will attempt to identify the type of OS installed on the device.

For details about the discovery criteria and the columns included in each discovery view, see the following tables.

Table 1. Discovery criteria

View	Description
AD and SIM computers	Lists all computers that have been found using Active Directory discovery, or that have been reported via the Snow Integration Manager (SIM). The view includes both reachable and unreachable computers.
Reachable network devices	Lists all devices that support SNMP but have not been identified as computers, for example printers, switches, and routers.
Reachable unknown devices	Lists all devices that are reachable but for which no additional information can be gathered.
Reachable computers	Lists all devices that have been identified as computers using one (or several) of the discovery methods WinRPC/WMI, TCP/IP fingerprinting, or Active Directory discovery.
Reachable computers with Snow Inventory Client 3.x for Windows	Lists all reachable Windows computers/devices that have not been upgraded yet, and that still have the old Inventory client installed.

Table 2. Columns included in each discovery view

	AD and SIM computers	Reachable network devices	Reachable unknown devices	Reachable computers	Reachable computers with Snow Inventory Client 3.x for Windows
Hostname	X	-	-	X	-
Platform Example: Windows	X	-	-	X	-

	AD and SIM computers	Reachable network devices	Reachable unknown devices	Reachable computers	Reachable computers with Snow Inventory Client 3.x for Windows
Site name Example: SESTOSOL-05	X	X	X	X	X
Last logon (AD)	X	-	-	X	-
Is reachable Example: Yes	X	-	-	-	-
Source Example: Active Directory	X	-	-	-	-
Last updated	X	X	X	X	X
IP Address	-	X	X	X	X
MAC Address	-	X	X	X	X
Description Example: HP ETHERNET MULTI-ENVIRONMENT	-	X	X	-	X
NIC manufacturer Example: Hewlett Packard	-	X	X	-	-
Type Example: Network	-	-	-	-	X

To change the columns included in a selected discovery view, create a custom view by copying it and then adding (or removing) columns to it. Also, filter criteria can be added to the custom view. For details, see Work with views.

3.3.2.1 Snow Active Directory Discovery service

Customers that use the previous Snow Active Directory Discovery service for gathering of Active Directory information can continue to do so in the Inventory 5 environment. However, the service instances need to be configured to use the following web API on the Inventory 5 server (Master Server or Service Gateway) for delivery of the discovery result:

http://hostname:port/legacy/ActiveDirectoryDiscovery.asmx

For configuration, see the document *Snow Active Directory Discovery, User guide*.

NOTE

- The Snow Active Directory Discovery service cannot run on the same server as Inventory 5. This means, if the service is installed on a Inventory 3 server that is to be upgraded to Inventory 5, it needs to be uninstalled prior to the upgrade.
- The web API is the only supported delivery method for this discovery result. Delivery to folders on local disks or network shares is not supported.

3.4 SYSTEM EVENTS

On the **System Events** page tasks like agent scans and agent deployments (Windows) are logged.

3.4.1 COMMANDS

The following commands are available on the **System Events** page:

Command	Description
Export	Export the information as it is displayed in the **System Events** view to file. Any grouping or sorting will apply.
Search	Show (or hide) the search box
Refresh	Refresh the content of the view
Show details	View details of a selected event
Pause event	Pause a running event
Delete	Delete a system event

3.4.1.1 SYSTEM EVENT DETAILS

To see details of a specific system event, double-click the event or select the event in the list and then click **Show details**.

A summary is displayed in the main window, and a container for the event is added under **System Events** in the category structure. Expand each of the icons **Successful**, **Pending**, **Failed**, and **Total** to have the details presented in the main window.

3.5 AGENT UPDATES

The **Agent updates** page lists all updates that have been made to the agents, such as configuration updates and updates of support files.

When an agent update is created, criteria are set for which devices that the agent will target. When the update has been created, it will be continuously looking for devices that match the configured criteria. This ensures that any new devices that show up in the organization will be updated as well.

The option **Allow downgrade of agent version** will decide whether the update is allowed to install an earlier agent (with a lower version number) or not.

NOTE

- An active agent update will have the status **In progress** in the **Agent updates** view, even if no actual update is running at the moment.
- An agent update will be indicated as successful if it completes its task without failure. For example, if an agent update with the **Allow downgrade of agent version** option disabled (not selected) targets a computer with a higher agent version number, the update will be marked as successful even though no actual update was made.

3.5.1 COMMANDS

The following commands are available on the **Agent Updates** page:

Command	Description
Export	Export the information as it is displayed in the **Agent updates** view to file. Any grouping or sorting will apply.
Search	Show (or hide) the search box
Refresh	Refresh the content of the view
Show details	View details of a selected agent update, including targets of the update
Create new	Create a new agent update using the **Create new update** wizard
Pause update / Resume update	Pause an active agent update / resume a paused agent update
Delete	Delete an agent update

3.5.1.1 AGENT UPDATE DETAILS

To see details of a specific agent update, double-click the update or select the update in the list and then click **Show details**.

A summary is displayed in the main window, and a container for the update is added under **Agent Updates** in the category structure. Expand each of the icons **Successful**, **Pending**, **Failed**, and **Total** to have the details presented in the main window.

3.6 CONFIGURATIONS

The **Configurations** page lists all configurations that have been identified on the inventoried devices. The **Published** column reflects if the configuration has been created and deployed via the Admin Console (**Yes**) or not (**No**).

When a new (or updated) configuration is saved and deployed, it is sent as a one-time job to all computers with that configuration that are known at that particular point in time. To have the configuration sent to any new computers that might show up later on, create an agent update instead and add the configuration file as a support file.

Agent configuration templates for all platforms are provided via the Snow Update Service (SUS). They are downloaded to the Snow Inventory Master Server by the SUS client and, by default, put in the folder:

%ProgramData%\SnowSoftware\Inventory\Resources\Agent Configuration Templates

3.6.1 COMMANDS

The following commands are available on the **Configurations** page:

Command	Description
Export	Export the information as it is displayed in the **Configurations** view. Any grouping or sorting will apply.
Search	Show (or hide) the search box
Refresh	Refresh the content of the view
Show details	View details of a selected configuration
Create new	Create a new configuration
Edit	Edit a selected configuration
Copy	Copy a selected configuration, and save it with another name
Delete	Delete a selected configuration
Export to file	Export a selected configuration to file
Import from file	Import a configuration from file

3.6.1.1 CONFIGURATION DETAILS

To see details of a specific configuration, double-click the configuration or select the configuration in the list and then click **Show details**.

A summary is displayed in the main window, and a container for the configuration is added under **Configurations** in the category structure.

3.7 INVENTORY SERVERS

On the **Inventory Servers** page all servers in the Inventory platform are presented: Database server, Master servers, and Service gateways.

3.7.1 COMMANDS

The following commands are available on the **Inventory Servers** page:

Command	Description
Export	Export the information as it is displayed in the **Inventory Servers** view to file. Any grouping or sorting will apply.
Search	Show (or hide) the search box
Refresh	Refresh the content of the view
Show details	View details of a selected Inventory server

3.7.1.1 Server details

To see details of a specific Inventory server, double-click the server or select the server in the list and then click **Show details**.

A summary is displayed in the main window, and a container for the server is added under **Inventory servers** in the category structure.

The **Discovery interfaces** section shows whether or not the network interface exists and is turned on (**Active** = **Yes** / **No**), and is configured for discovery (**Enable**= **Yes** / **No**). Discovery will only be performed for interfaces that are both **Active** and **Enabled**.

To configure a network interface for discovery, see Manage Discovery configuration.

4 STEP-BY-STEP INSTRUCTIONS

4.1 CREATE A NEW CONFIGURATION

1. In the category menu, click **Configurations**.
2. Click **Create new.**
   The **New configuration** wizard appears.

4.1.1 GENERAL

On the **General** page:

1. Type a **Name** of the new configuration.
2. Type a **Site name** for the new configuration, or select an existing site in the list.

4.1.2 SERVER

On the **Server** page, add the Snow Inventory servers that the computers with this configuration can communicate with. Add one or several servers.

1. Click **Add**.
   The **Server** dialog box appears.
2. Type a server **Address**, or select an existing address in the list. When typing a new address, the server address must be in the following format:
   - http://[server name]:[port]/
3. Optionally in the **Proxy settings** section, type a **Server** name along with a **User name** and **Password** for accessing the proxy server.
4. Optionally in the **Client certificate** section, type a **File path** to the certificate and the **Password** for the private key.
5. Click **Add** to add the server and close the **Server** dialog box.
   The server is added to the list.

4.1.3 SCHEDULE

NOTE

- The settings on the **Schedule** page only apply to the Windows agent. The other agents do not handle scheduling via the configuration file, and will ignore any settings made here.

On the **Schedule** page, set a time and an interval for when clients with this configuration will run a scan. Use the **Randomization** functionality to spread the start time of the scan among the agents. The agents will then run a scan at a randomly selected time 90 minutes (default) after the defined **Time of day**.

EXAMPLE
The scan is set to start at 09:00 with a default randomization of 90 minutes. This means that the agent randomly will select a start time for the scan between 09:00 and 10:30.

To add a schedule:

1. Click **Add**.
   The **Schedule** dialog box appears.
2. Select **Schedule** interval in the list.
   - For the **Daily** schedule, also set **Time of day**.
     Optionally, select the **Randomization** check box.
   - For the **Weekly** schedule, also set **Weekday** and **Time of day**.
     Optionally, select the **Randomization** check box.
   - For the **Monthly** schedule, also set **Day** and **Time of day**.
     Optionally, select the **Randomization** check box.
3. Click **Add** to save the changes and close the **Schedule** dialog box.
   The schedule is added to the list.

4.1.4 SOFTWARE SETTINGS

On the **Software settings** page settings can be made for what directories, file systems, and file types to include in, or exclude from, the scan. All **Include** and **Exclude** rules use wildcard matches, so use * for unknown characters.

In the **Include** section:

- Use the **Recursive** functionality to scan subdirectories of the specified directory
- For Unix, use the **Unconditional** functionality to include all files. This will override any settings that have been defined for **Exclude**.
- For Windows, use the check box to select whether or not to **Include software information from any locally attached (or mounted) disk**.

NOTE

- A value must be set for the **Include** command, or no scan will run.
- For the Snow Inventory Agents for Linux and macOS, some file systems are excluded from the scan by default, and cannot be included using include criteria. For detailed information, refer to the *Configuration Guide, Snow Inventory Agents*.

4.1.4.1 INCLUDE

In the **Include** section, specify all directories to be included in the scan. Repeat the steps for all directories to be included.

1. Click **Add**.
   The **Include** dialog box appears.
2. In the **Path** box, type a directory by specifying it from the root.
3. When applicable, select the **Recursive** check box.
4. When applicable, select the **Unconditional** check box.
5. Click **Add** to save and close the **Include** dialog box.

4.1.4.2 Include criteria - File system

In the **File system** section, specify all file systems to be included in the scan. Repeat the steps for all file systems to be included.

1. Click **Add**.
   The **Include criteria** dialog box appears.
2. In the **File system** box, type the file system to be included.
3. Click **Add** to save and close the **Include criteria** dialog box.

4.1.4.3 Include criteria - File type

In the **File type** section, specify the file types to be included in the scan. Repeat the steps for all file types to be included.

1. Click **Add**.
   The **Include criteria** dialog box appears.
2. In the **File type** box, type the file type to be included.
3. Click **Add** to save and close the **Include criteria** dialog box.

4.1.4.4 Exclude - Path

In the **Exclude** section, specify the directories to be excluded from the scan. Repeat the steps for all directories to be excluded.

1. Click **Add**.
   The **Exclude** dialog box appears.
2. In the **Path** box, type a directory by specifying it from the root.
3. Click **Add** to save and close the **Exclude** dialog box.

4.1.4.5 Exclude – File system

In the **Exclude** section, specify the file systems to be excluded from the scan. Repeat the steps for all file systems to be excluded.

1. Click **Add**.
   The **Exclude** dialog box appears.
2. In the **File system** box, type the file system to be excluded.
3. Click **Add** to save and close the **Exclude** dialog box.

4.1.5 LOGGING

On the **Logging** page, general log settings for the inventory scan and system events can be set.

4.1.5.1 Inventory scan log

1. Select **Log level** in the list.
2. Type a **Max log size** in the box.
3. To log external tasks that are run with elevated privileges, select the **Privileged operation (privop)** check box.

NOTE
The log file is by default cleared before a new scan is started. Use the system setting **log.append** to have new log entries appended to the log file instead.

4.1.5.2 System log

1. To enable logging to the system event log, select the **Enable system logging** check box.
2. Select **Log level** in the list.
3. To log external tasks that are run with elevated privileges, select the **Privileged operation (privop)** check box.

4.1.6 DROP LOCATION

On the **Drop Location** page, select how the agent will deliver the result files of the inventory scan. Configure one or several drop locations.

4.1.6.1 Networks

Add a location on another client computer on the network:

1. Click **Add**.
   The **Drop networks** dialog box appears.
2. Type a network **Location** in the box.
   Example: **\\[servername]** or **\\[ip address]**
3. Type information on **User name** and **Password** for accessing the network location.
4. Click **Add** to save and close the **Drop networks** dialog box.

4.1.6.2 Paths

Add a path on the client computer:

1. Click **Add**.
   The **Drop paths** dialog box appears.
2. Type the folder **Path** in the box.
3. Click **Add** to save and close the **Drop paths** dialog box.

4.1.6.3 Endpoints

Add an Inventory server (Master Server or Service Gateway):

1. Click **Add**.
   The **Endpoints** dialog box appears.
2. Type the server **Address** including port number.
   Example: **http://[servername]:[port]** or **https://[servername]:[port]**
3. Optionally in the **Proxy settings** section, type a **Server** name along with a **User name** and **Password** for accessing the proxy server.
4. Click **Add** to save and close the **Endpoints** dialog box.

4.1.7 DENY

NOTE

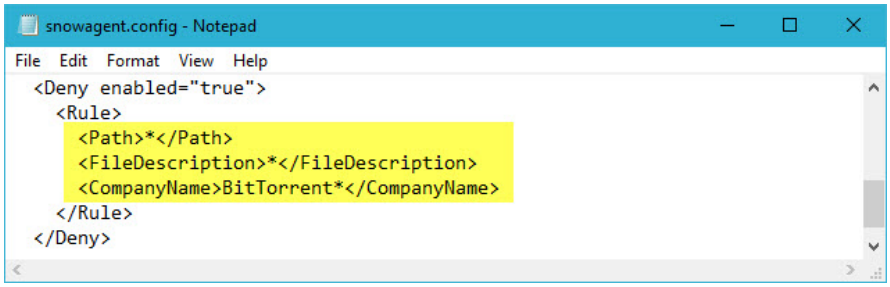
- The settings on the **Deny** page only apply to the Windows agent.

On the **Deny** page, one or several rules can be defined to prevent certain software, such as inappropriate or illegal software, from running on the client computers.

When a rule is created a **Path**, a **File description**, and a **Company name** (manufacturer name) of the software executable must specified. If any of these properties is unknown or could be multiple, use * as a wildcard character. However, at least one of the three properties must be specified.

EXAMPLE

- A filter that will prevent Notepad from being used (this is only an example for testing purposes, it is not a practical one):
  Path = C:\Windows\System32\notepad.exe
  File description = *
  Company name = *
- A filter that will prevent any software that is described as "poker" software from being used:
  Path = *
  File description = *poker*
  Company name = *
- A filter that will prevent any software from a company with a name that starts with "BitTorrent" from being used:
  Path = *
  File description = *
  Company name = BitTorrent*
  This last example will result in the following lines in the agent configuration file (snowagent.config):



To enable the deny rules and add software:

1. Select the **Enable deny rules** checkbox.
2. Click **Add** .
   The **Deny** dialog box appears.
3. Type the directory **Path** to the software executable.

   EXAMPLE
   C:\Windows\System32\notepad.exe

4. Type the **File description** of the software executable.
   To find the file description; right-click the the executable, select **Properties** , and then look for the **Description** on the **General** tab.

   EXAMPLE
   Notepad

5. Type the **Company name** of the software manufacturer.
   To find the company name; add the **Company** column to the File explorer view of the folder where the executable is located.

   EXAMPLE
   Microsoft Corporation

6. Click **Add** to save and close the **Deny** dialog box.

NOTE
The Snow Inventory Agent will monitor system processes where blocked (denied) applications are launched. The agent will not prevent the blocked application from being launched, but after a short while it will end the process and the application will close.

4.1.8 ORACLE

NOTE

- The settings on the **Oracle** page only apply to the Linux, Unix, and Windows agents.

On the **Oracle** page, settings can be made for running a scan in an Oracle environment. Default credentials for Oracle access can be set while, if any, specific credentials required for a certain Oracle instance are set on the instance directly.

Select to scan **All instances**, or specify the instances individually in the **Include** section. Another option is to enable the **All instances** option, and then specify instances to exclude from the scan.

To enable an Oracle scan:

- Select the **Enable Oracle scan** check box.

In the **Default credentials** section:

1. Type information on **User name** and **Password** for accessing the Oracle environment.
2. Select whether to include **All instances** in the scan, or to specify the instances individually.

In the **Include instances** section, it is possible to specify and include instances individually. To include an individual Oracle instance:

1. Click **Add**.
   The **Include instance** dialog box appears.
2. Type the Oracle **Sid** and Oracle **Home** for the instance.
3. If specific credentials are required, type information on **User name** and **Password** for accessing the instance.

4. Click **Add** to save and close the **Include instance** dialog box.

In the **Exclude instances** section, it is possible to excluded instances from the scan, when the **All instances** option is enabled. To exclude an individual Oracle instance:

1. Click **Add**.
   The **Exclude instance** dialog box appears.
2. Type the **Sid** for the instance to be excluded.
3. Click **Add** to save and close the **Exclude instance** dialog box.

4.1.9 SYSTEM SETTINGS

On the **System Settings** page, a number of low level system variables can be set.

For information on functionality of each respective system setting, refer to the document *configuration–doc.html* that is included in the agent installation files.

NOTE

- System variables should be used with caution.

To set a system variable:

1. Click **Add**.
   The **System setting** dialog box appears.
2. Select **Key** from the list.
3. Use the **Value** checkbox for Boolean variables, or type a **Value** in the box.
4. Click **Add** to save and close the **System setting** dialog box.

4.2 EXPORT CONFIGURATION TO FILE

1. In the category view, click **Configurations**.
2. In the list of configurations, select the configuration to export and then click **Export to file**.
   The **Save as** dialog box appears.
3. Browse for a location where to store the configuration file.
4. Type a **File name**
5. Verify that **Save as type** is set to **Configuration (*.config)**.
6. Click **Save**.

4.3 CREATE A NEW AGENT UPDATE

1. In the category view, click **Agent updates**.
2. Click **Create new**.
   The **Create new update** wizard appears.

4.3.1 GENERAL

On the **General** page:

1. Type a **Name** and a **Description** of the new update.
2. Select the **Target operating system** that the agent update will be created for.

4.3.2 CONTENT

An agent update could consist of a new version of the agent, support files to be updated, support files to be removed, or all three scenarios. A support file could, for example, be a PowerShell script.

NOTE

- A configuration file can be sent to the agent as a support file. In that case the file name of configuration file must be set to **snowagent.config**.

To include a new version of an agent:

1. Select the **Install agent** check box, and then select agent version in the list.
2. To allow for installation of an older version than the currently installed, select the **Allow downgrade of agent version** check box.

To include new support files:

1. In the **Add support files** section, click **Add**.
   The file browser appears.
2. Browse for the file to be added, and then click **Open**.
   The file is added to the **File** list.

   NOTE
   PowerShell scripts provided via Snow Update Service (SUS) can, by default, be found in this folder on the Master Server:

   %ProgramData%\SnowSoftware\Inventory\Resources\Powershell Scripts

To remove an existing support file from the agent:

1. In the **Delete support files** section, click **Add**.
   The **Delete support file** dialog box appears.
2. Type the name of the file to be deleted, and then click **Add**.
   The file is added to the **File** list.

4.3.3 TARGETS

Select where to find the targets of the agent update by specifying one or more sites.

1. In the **Site(s)** section, click **Add**.
2. Select a site in the list, and then click **Add**.
   The site is added to the **Site** list.
3. To add all sites to the list, click **Add all**.

By default, all devices in the site will be target for the update. To target a subset of the devices, use the **Configurations**, **Devices**, or **View** options.

4.3.3.1 CONFIGURATIONS

1. In the **Subset** section, select the **Configurations** option.
2. In the **Configurations** section, click **Add**.
3. Select a configuration in the list, and then click **Add**.
   The site is added to the **Configurations** list.

4.3.3.2 DEVICES

1. In the **Subset** section, select the **Devices** option.
2. In the **Devices** section, click **Add**.
3. Type a device name in the **Add device** box, and then click **Search**.
4. In the search result list, click the device, and then click **Add**.
   The device is added to the **Devices** list.

4.3.3.3 VIEW

1. In the **Subset** section, select the **View** option.
2. Select a **View** in the list.

4.3.4 SCHEDULING

The server will inform the agent that there is an update available. The agent will download the update immediately, but will wait to install it as configured here.

1. In the **Start time** section, set a date and time for when the server will notify the agents that that there is an update available.
2. To configure a time frame for when the agent can run the update, select the **Use local service window** check box and set **Start time** and **End time**.

4.3.5 SUMMARY

In the last step, a **Summary** of all settings is displayed. Click **Publish** to activate the agent update, or click **Previous** to go back and make any changes in the settings.

4.4 DEPLOY AN AGENT

The Snow Inventory Agent for Windows can be deployed to discovered objects via the Admin Console. Also, with the deployment it is possible to have any currently installed Snow Inventory Client for Windows (3.x) removed from the object.

NOTE

- The user account that performs the deployment needs to have either Local administrator or Domain administrator privileges. By default, the deployment is run by the account that runs the Inventory server.
- If the hostname of the target is not known, Domain administrator privileges are required.
- File and Printer Sharing must be enabled on the target computer.
  In the Windows Firewall, the following ports need to be open on the target computer:
  - UDP 137 and 138
  - TCP 139 and 445

  NOTE
  These ports are disabled by default in the Windows Server operating systems.

- The target must accept Windows RPC connections.

To deploy an agent:

1. In the category view, click **Discovery**.
2. Select an object in the list, and then click **Create deployment**.
   The **Create deployment** dialog box appears.
3. In the **Site name** list, select the site where the configuration can be found.
4. In the **Configuration** list, select which configuration to deploy to the object.
   Available configurations depend on selected site (previous step).
5. In the **Inventory Agent** list, select which agent package to deploy to the object.
   Available packages depend on selected configuration (previous step).
6. Optionally, type credentials of a user account with administrative privileges in the **Domain**, **User name**, and **Password** boxes.
   If no credentials are provided, the account that runs the Inventory server service will be used.
7. To have any currently installed Snow Inventory Client for Windows removed from the object, select the **Remove legacy client** check box.
8. Click **Deploy** to save the changes and close the **Create deployment** dialog box.
   The new deployment is listed in the **System Events** view.

4.5 DEPLOY THE SNOW INVENTORY ORACLE SCANNER

NOTE

- All agents (Windows, Linux, macOS, Unix and SIOS) are updated through the Snow Update Service (SUS). By default, all agent files are stored in the **C:\ProgramData \SnowSoftware\Inventory\Resources\Agent** folder on the Inventory server.
- The Snow Inventory Oracle Scanner (SIOS) requires that one of the other three agents (Windows, Linux, or Unix since Oracle Database cannot be installed on macOS) is installed along with it. Technically, the **sios.jar** file is a regarded a "support file" that needs to be put in the same folder as the **snowagent.exe** file.

4.5.1 UPGRADE AN EXISTING SIOS INSTALLATION

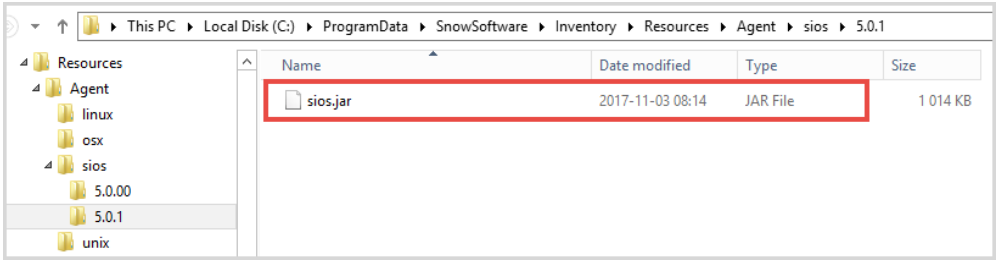
To deploy a higher version of SIOS to a client computer that already has SIOS installed, create an agent update job and include the **sios.jar** file as a support file.

The following instruction will take you through the steps. To see a more detailed instruction of how to create a new agent update, refer to Create a new agent update.

To upgrade an existing SIOS installation, do this:

1. Verify that the latest **sios.jar** file has been downloaded to the Inventory server by SUS.

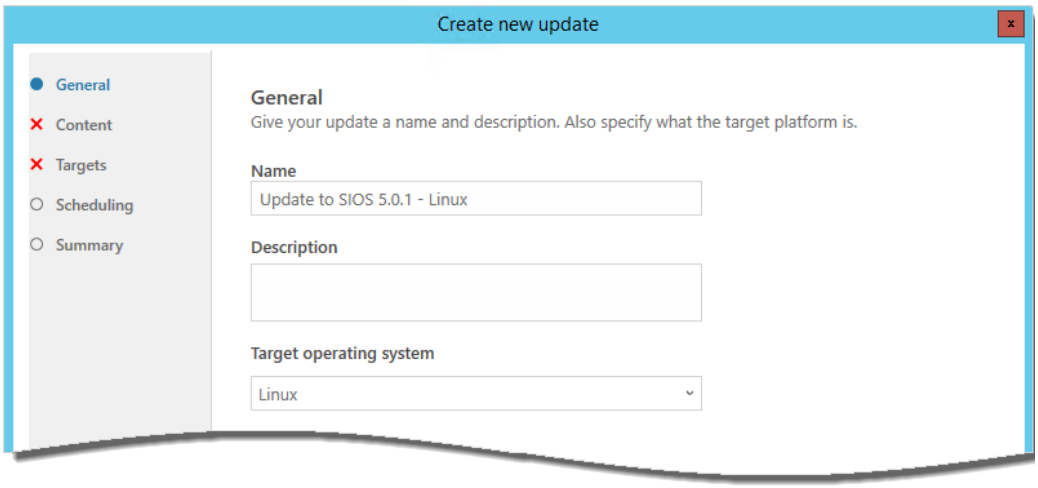
   EXAMPLE
   In this example, the **sios.jar** file for SIOS version 5.0.1 exists in the **C:\ProgramData \SnowSoftware\Inventory\Resources\Agent\sios\5.0.1** path.

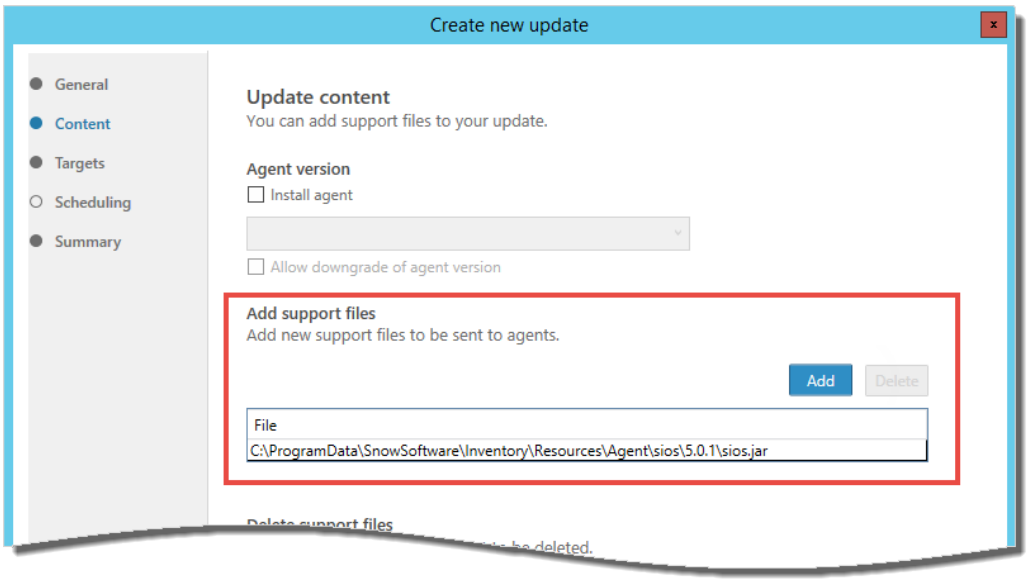
   If no such file or directory exists, make sure to run SUS to download the latest versions of the Inventory agents.

2. In the **Inventory Server Admin Console**, navigate to the **Agent Updates** view, and then click **Create new**.

3. On the **General** page:
    1. Type an appropriate **Name** of the new update.
    2. Select the **Target operating system** that the agent update will be created for.
    3. Click **Next**.

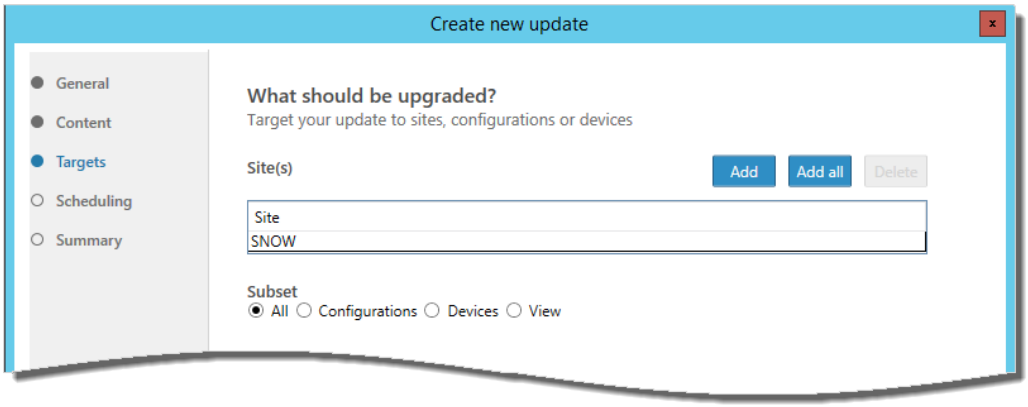


4. On the **Content** page:
    1. In the **Add support files** section, click **Add** and then browse for the **sios.jar** file (see step 1).
    2. Click **Next**.

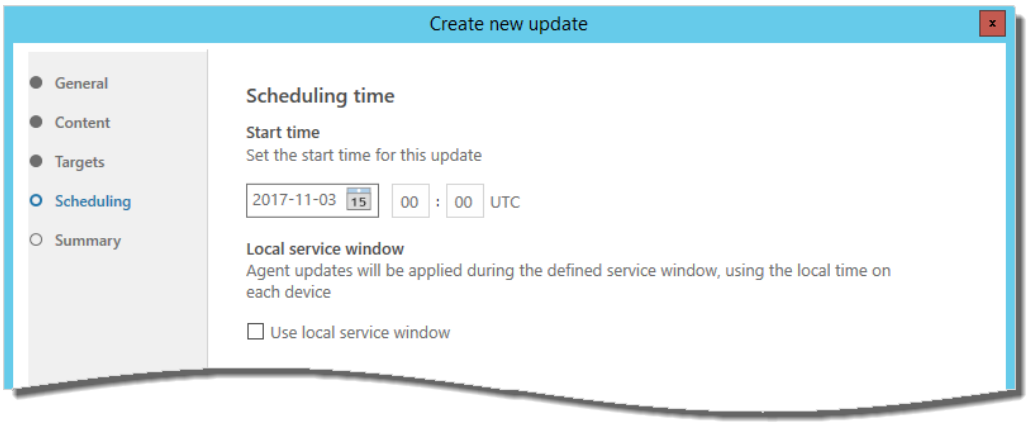


5. On the **Targets** page:

    1. Specify in what **Site** the targets of the update are to be found.
    2. By default, **All** devices in that site will be targets for the update. To target a subset of the devices, use the **Configurations**, **Devices**, or **View** options.
    3. Click **Next**.



6. On the **Scheduling** page, decide either to publish the update immediately or to schedule it to a future date and time, for example an upcoming service window. To publish the update immediately, just click **Next**.



7. On the **Summary** page, verify that the settings are correct, and then click **Publish**.
8. The agent update is now published. The targeted agents will automatically upgrade themselves the next time they connect to the Inventory server. Follow the update progress in the **Agent updates** view of the Admin Console.

4.5.2 INSTALL SIOS FOR THE FIRST TIME

To deploy SIOS to a client computer that doesn't yet have SIOS installed, create an agent update job and include both a **configuration** file and the **sios.jar** file as support files. The configuration needs to include settings for the Oracle scan.

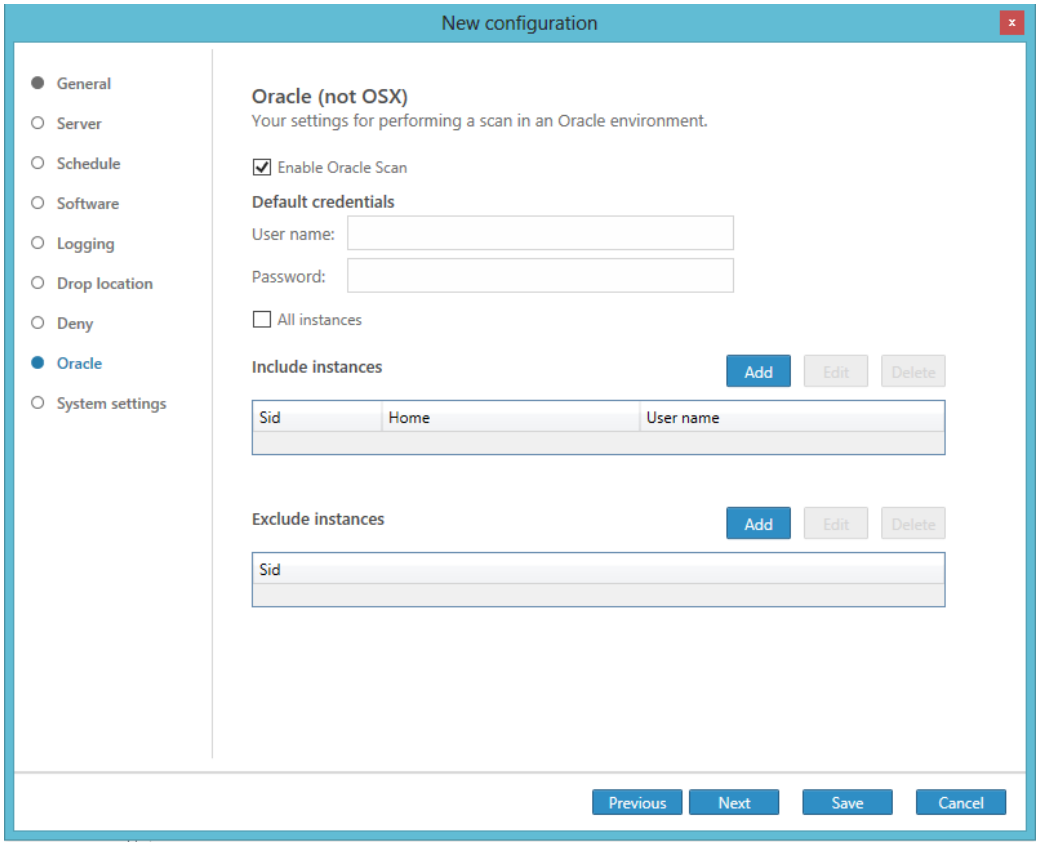
The following instructions will take you through the steps. To see a more detailed instruction of how to create a new configuration and a new agent update, refer to Create a new configuration and Create a new agent update.

NOTE

- You need to create one configuration file for each operating system type for which you want to perform an Oracle scan.
- Use an existing configuration for the operating system type as template by copying it in the Admin Console.

To copy an existing configuration:

1. In the **Inventory Server Admin Console**, navigate to the **Configurations** view.
2. In the list of existing configurations, select the configuration to be copied, and then click **Copy**.
3. Give the configuration an appropriate name for easy identification.
4. On the **Oracle** page, click the **Enable Oracle scan** check box.
   Then, make the settings for running a scan in your Oracle environment.
   For detailed information on the settings, refer to Oracle.



5. Save the new configuration for SIOS.

To export the new configuration to file:

1. In the **Configurations** view, select the new configuration for SIOS, and then click **Export to file**.
2. Browse for a location where to save the file and type an appropriate **File name**.
3. Verify that the file type is set to **Configuration (*.config)**, and then click **Save**.

To create an agent update containing the **configuration** file and the **sios.jar** file:

1. In the **Agent updates** view, click **Create new**.
2. Follow the instructions in the Upgrade an existing SIOS installation section.

   NOTE

   On the **Content** page, add both the new **configuration** file and the **sios.jar** file as support files.

4.6 ENABLE CLOUD APPLICATION DISCOVERY AND METERING

1. In the menu, click **Cloud App Metering**.
   The **Cloud Applications Metering Configuration** dialog appears.
2. Click **Add**.
   The **Sites and Configurations** dialog box appears.
3. In the **Selected site** list, select a site where the feature will be enabled.
4. In the **Available configurations** list, select one or more agent configurations for which the feature will be enabled.
5. Click **Add** to save the settings and close the **Sites and Configurations** dialog box.
   Selected site and agent configurations are added to the list.

4.7 IMPORT CONFIGURATION FROM FILE

1. In the category view, click **Configurations**.
2. Click **Import from file**.
   The **New configuration** wizard appears.

On the **Import** page:

1. Click **Import configuration**.
   The **Open** dialog box appears
2. Browse to select the configuration file to import, and then click **Open**.

   NOTE
   Agent configuration templates provided via Snow Update Service (SUS) can, by default, be found in this folder on the Master Server:

   %ProgramData%\SnowSoftware\Inventory\Resources\Agent Configuration Templates

3. Click **Next**.

On the **General** page:

1. Type a **Name** of the new configuration.
2. Type a **Site name** for the imported configuration, or select an existing site in the list.

3. Click **Next**.

On the following pages, the information in the configuration file is displayed. Click through the pages to verify the configuration.

Click **Save** the save the imported configuration and close the **New configuration** wizard.

4.8 MANAGE DISCOVERY CONFIGURATION

NOTE

- "Ping" discovery will always be performed for any defined IP address range.

4.8.1 NETWORK DISCOVERY

An Inventory server can be configured to perform network discovery on specific IP address ranges using the following technologies: SNMP, SSH, WinRPC/WMI, ICMP, DNS lookup, TCP/IP fingerprinting, and NIC manufacturer lookup.

NOTE

- When using TCP/IP fingerprinting, the ports of the Inventory server must be opened for all incoming TCP/IP traffic destined for the application **snowserver.exe**.

4.8.1.1 ADD NETWORK DISCOVERY

1. In the category view, click **Inventory servers**.
2. Select a server in the list, and then click **Show details**.
3. Click **Edit**.
   The **Server Discovery options** wizard appears.
4. Click **Device discovery**.
   The **Device discovery options** page appears.
5. In the **Network discovery options** section, click **Add**.
   The **Add network discovery** dialog box appears.
6. Select **Interface** in the list.
   The IP range boxes **From** and **To** are automatically populated with a suggested address range of the selected interface.

   NOTE

   - The range is only a suggestion and can be edited if need be.
   - IP addresses outside of the selected interface's subnet can also be included.
7. Enable the discovery methods to be used for the selected **Interface** and **IP range** by selecting **Enabled** in the respective lists.
   The **Ports** are set automatically to the standard ports, but can be changed.
8. Click **Add** to add the network discovery and close the **Add network discovery** dialog box.

The selected discovery methods are added to the list.

9. Click **Save** to save the changes and close the **Server Discovery options** wizard.

4.8.1.2 Edit Network discovery

1. In the category view, click **Inventory servers**.
2. Select a server in the list, and then click **Show details**.
3. Click **Edit**.
   The **Server Discovery options** wizard appears.
4. Click **Device discovery**.
   The **Device discovery options** page appears.
5. In the **Network discovery options** section, select an **Interface** in the list, and then click **Edit**.
6. Make the changes.
7. Click **Update** to update the network discovery and close the **Add network discovery** dialog box.
8. Click **Save** to save the changes and close the **Server Discovery options** wizard.

4.8.2 ACTIVE DIRECTORY DISCOVERY

An Inventory server can be configured to perform Active Directory discovery using LDAP or secure LDAP. Information on both devices and users can be gathered, and multiple LDAP paths can be configured.

NOTE

- Depending on the size of the network to be discovered, it will take some time for the devices to appear in the **Discovery** view of the Admin Console.
- Information on users will be gathered and stored in the Inventory Server database, but it will not be visible in the user interface of the Admin Console.

4.8.2.1 Enable Active Directory discovery of computers

NOTE

- When enabling Active Directory discovery of computers for the domain which the Snow Inventory Master server is member of, **User Name** and **Password** need not to be provided. However, when using secure LDAP user credentials are required.

1. In the category view, click **Inventory servers**.
2. Select a server in the list, and then click **Show details**.
3. Click **Edit**.
   The **Server Discovery options** wizard appears.
4. Click **Device discovery**.
   The **Device discovery options** page appears.
5. In the **Active Directory discovery options** section, select the **Enable Active Directory device discovery** check box.

6. In the **Active Directory discovery options** section, click **Add**.
   The **Add LDAP Path** dialog box appears.
7. Type an **LDAP path** to the Active Directory domain.
   If a specific port is required, specify it in the LDAP path.

   EXAMPLE

   - The Inventory Server is a member of the domain to be scanned:
     ldap://CN=Computers,DC=MyDomain,DC=com
   - The Inventory Server is not a member of the domain to scanned:
     ldap://DC001.MyDomain.com
     ldap://DC001.MyDomain.com/CN=Computers,DC=MyDomain,DC=com
8. To use secure LDAP, select the **Use SSL** check box.
9. Type a **User Name** of a user with read privileges in the Active Directory domain.
   Use the following format: *domain\username*
10. Type and confirm the **Password** of the user.
11. Click **Add**.
    The LDAP path is added to the list.
12. Click **Save** to save the changes and close the **Server Discovery options** wizard.

4.8.2.2 Edit Active Directory discovery of computers

1. In the category view, click **Inventory servers**.
2. Select a server in the list, and then click **Show details**.
3. Click **Edit**.
   The **Server Discovery options** wizard appears.
4. Click **Device discovery**.
   The **Device discovery options** page appears.
5. Make the changes in the **Active Directory discovery options** section.
6. Click **Save** to save the changes and close the **Server Discovery options** wizard.

4.8.2.3 Enable Active Directory discovery of users

NOTE

- When enabling Active Directory discovery of users for the domain which the Snow Inventory Master server is member of, **User Name** and **Password** need not to be provided. However, when using secure LDAP user credentials are required.

1. In the category view, click **Inventory servers**.
2. Select a server in the list, and then click **Show details**.
3. Click **Edit**.
   The **Server Discovery options** wizard appears.
4. Click **User discovery**.
   The **User discovery options** page appears.

5. Select the **Enable Active Directory user discovery** check box.
6. Click **Add**.
   The **Add LDAP Path** dialog box appears.
7. Type an **LDAP path** to the Active Directory domain.
   If a specific port is required, specify it in the LDAP path.

   EXAMPLE

   - The Inventory Server is a member of the domain to be scanned:
     ldap://CN=Users,DC=MyDomain,DC=com
   - The Inventory Server is not a member of the domain to scanned:
     ldap://DC001.MyDomain.com
     ldap://DC001.MyDomain.com/CN=Users,DC=MyDomain,DC=com
8. To use secure LDAP, select the **Use SSL** check box.
9. Type a **User Name** of a user with read privileges in the Active Directory domain.
   Use the following format: *domain\username*
10. Type and confirm the **Password** of the user.
11. Click **Add**.
    The LDAP path is added to the list.
12. Click **Save** to save the changes and close the **Server Discovery options** wizard.

4.8.2.4 Edit Active Directory discovery of users

1. In the category view, click **Inventory servers**.
2. Select a server in the list, and then click **Show details**.
3. Click **Edit**.
   The **Server Discovery options** wizard appears.
4. Click **User discovery**.
   The **User discovery options** page appears.
5. Make the changes.
6. Click **Save** to save the changes and close the **Server Discovery options** wizard.

4.9 WORK WITH VIEWS

Custom views can be added, edited, and deleted on the **Devices** and the **Discovery** pages. A custom view can be created from scratch or by copying an already existing view.

4.9.1 ADD VIEW

To add a view:

- Click **Add view**.
  The **View editor** wizard appears.

4.9.1.1 Name

On the **Name** page, type a **Name** for the view.

4.9.1.2 COLUMNS

On the **Columns** page, select which columns to show in the view:

1. Scroll the list or type the information to search for in the **Available columns** box.
   The search result is then displayed in the list below.
2. Include all parameters by selecting a category, or expand the category to only select a certain parameter.
3. Click  to add the column to the view.
   The selected information is moved to the **Selected columns** list.
4. Repeat for all required columns.

4.9.1.3 FILTER

On the **Filter** page, optionally add one or more filter criteria for the view:

1. Select what to filter for in the **Show rows** where list.
2. Select operator, and set value (when applicable).
3. Click  to add another criterion, or click **Add group** to add a group of criteria.
4. Click **Save** to save the view and close the **View editor** wizard.

4.9.2 EDIT VIEW

NOTE

- Only custom views can be edited.

1. Select the view in the list, and then click **Edit view**.
   The **View editor** wizard appears.
2. Make the changes.
3. Click **Save** to save the changes and close the **View editor** wizard.

4.9.3 COPY VIEW

1. Select the view in the list, and then click **Copy view**.
   The **Save view as** dialog box appears.
2. Type a descriptive name of the view.
3. Click **OK** to save the copied view and close the **Save view as** dialog box.

4.9.4 DELETE VIEW

NOTE

- Only custom views can be deleted.

1. Select the view in the list and click **Delete view**.

2. A message is displayed where the deletion needs to be confirmed.
3. The view is removed from the list.

4.10 EXPORT VIEWS

The export functionality can be used in most views of the Admin Console. Data can be exported to Excel or CSV files.

1. Click **Export**.
   The **Save as** dialog box appears.
2. Browse for a location where to store the file.
3. Type a **File name** and select file type in the **Save as type** list.
4. Click **Save**.

4.11 MANAGE SYSTEM USERS

Each user of the Snow Inventory Admin Console needs a unique user account.

4.11.1 ADD USER ACCOUNT

1. In the menu, click **Settings**.
   The **Settings** dialog box appears.
2. Click **Users**.
   The **System users** page appears.
3. Click **Add.**
   The **User** dialog box appears.
4. Type a **User name** and a **Full name** for the new user account.
5. Type and confirm a **Password** for the new user account.
6. Click **Add** to create the user account and close the **User** dialog box.
7. Click **Save** to save the new user account and close the **Settings** dialog box.

4.11.2 DELETE USER ACCOUNT

1. In the menu, click **Settings**.
   The **Settings** dialog box appears.
2. In the **System users** view, select user in the list, and then click **Delete.**
   The user is removed from the list.
3. Click **Save** to save the changes, or click **Cancel** to undo the removal.
   The **Settings** dialog box is closed.

5 SNOW UPDATE SERVICE

The Snow Update Service (SUS) is used for updates of both server and agent files.

To use the Admin Console on a different server than the Master Server, the SUS root folder must be specified manually. Do the following:

1. In the menu, click **Settings**.
   The **Settings** wizard appears.
2. Click **Update service**.
   The **Update service root folder** page appears.
3. Click **Add**.
   The **SUS** dialog box appears.
4. Type the **Share path (UNC)** to the share where the update root folder is located.

   EXAMPLE

   - \\<computer name>\<share>
   - \\<computer IP address\<share>
5. Click **Add** to add the path and close the **SUS** dialog box.
6. Click **Save** to save the changes and close the **Settings** wizard.