Manage Your Device Inventory

About Device Inventory

DNA Center displays the device information gathered during the discovery process in the **Device Inventory** window. To access the **Device Inventory** window, from the DNA Center home page, click the **Device Inventory** tool.

DNA Center maintains the device inventory by polling the devices every 25 minutes. (The polling interval is set to 25 minutes by default, but you can change this setting to suit your network requirements.) Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than a day are displayed. This prevents any stale device data from being displayed. On an average, polling 500 devices takes approximately 20 minutes.

Table 1: Device Inventory Window Elements, on page 2 describes the main elements in the **Device Inventory** window.

For information about the actions that you can perform from the **Device Inventory** window, see Device Inventory Tasks, on page 7.

Table 1: Device Inventory Window Elements

Window Element	Description
Add Device	Discover a specific device and add it to your device inventory. If authentication of the device fails due to invalid credentials, the device enters a collection failure state. For information, see Add a Device Manually, on page 8.
⋮	Choose one of the following layouts or customize your own layout. For a list of the columns, see Table 2: Device Inventory Information, on page 3. • **Status—**Layout shows the **Device Name**, **IP Address**, **Reachability Status**, **Up Time**, **Last Updated Time**, **Poller Time**, and **Last Inventory Collection Status**. • **Hardware—**Layout shows the **Device Name**, **IP Address**, **MAC Address**, **IOS/Firmware**, **Platform**, **Serial Number**, **Last Inventory Collection Status**, **Config**, and **Device Family**. • **Tagging—**Layout shows the **Device Name**, **IP Address**, **MAC Address**, **Config**, **Device Role**, **Location**, and **Device Tag**.
Filters	Refine the list of devices that are displayed in the table by device name, IP address, last inventory collection status, and location. To remove or change the filters, click **Reset**.

The **Device Inventory** table displays the following information for each discovered device. All of the columns, except the **Config** column, support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

Table 2: Device Inventory Information

Column	Description
Device Name	Name of the device. Click the name to display the **Device Overview** dialog box with the following information: • **Name** • **IP Address** • **MAC Address** • **IOS Version** • **Up Time** • **Product Id** • **Associated WLC** • **Interface Name**, **MAC Address**, and **Status** of the interfaces on the device. **Note** The device name is displayed in red a device whose inventory has not been updated for more than 30 minutes.
IP Address	IP address of the device.

Column	Description
Reachability Status	State of the device. • **Connecting—**DNA Center is connecting to the device. • **Reachable—**DNA Center has connected to the device and is able to execute Cisco commands using the CLI . A failure indicates that DNA Center connected to the device, but was unable to execute Cisco commands using the CLI. This status usually indicates that the device is not a Cisco device. • **Authentication Failed—**DNA Center has connected to the device, but is unable to determine what type of device it is. This status also may indicate that the device is not a Cisco device. • **Unreachable—**DNA Center is unable to connect to the device. **Note** If credentials are not provided at the time a discovery request is made or earlier, the device status becomes **Not reachable**. You should perform a new discovery with the correct credentials.
MAC Address	MAC address of the device.
IOS/Firmware	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Up Time	Period of time that the device has been up and running.
Config	Configuration information. Click **View** to display detailed configuration information similar to what is displayed in the output of the **show running-config** command. **Note** This feature is not supported for access points and WLCs. Therefore, configuration data is not returned for these device types.

Column	Description
Device Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If DNA Center is unable to determine a device role, it sets the device role as unknown. **Note** DNA Center can change the device role as the network topology changes, but if you manually change the device role, then the role will not change as the network topology changes. If desired, you can use the drop-down list in this column to change the assigned device role. The following device roles are available: • Unknown • Access • Core • Distribution • Border Router
Location	Tag that you can apply to a device to denote its geographic location. By applying the same tag to several devices, you can group them based on a common attribute. The **Device Inventory** window and **Topology** window support location tags. Use the following guidelines when creating location tags: • Location tag information is maintained only in DNA Center and not deployed to or derived from the device itself. • A location defined in DNA Center is not the *civic-location* of the property that some devices support. • Location tags cannot be attached to hosts. • You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.

Column	Description
Device Tag	Tag assigned to devices to identify them by a common attribute. For example, you can create a tag and use it to group devices based on a platform ID or the Cisco IOS release. A number in the **Tag** column indicates how many tags have been applied to that device. **Note** You can use both a location tag and a device tag together. For information about adding or removing device tags, see Add or Remove a Device Tag in Device Inventory, on page 14. For information about deleting a tag, see Delete a Device, on page 15.
Policy Tag	Tag applied to a group of devices that will share the same policy.
Last Updated Time	Most recent date and time that DNA Center scanned the device and updated the database with new information about the device.
Device Family	Group of related devices, such as routers, switches and hubs, or wireless controllers.
Device Series	Series number of the device, for example, Cisco Catalyst 4500 Series Switches.
Last Inventory Collection Status	Status of the last discovery scan for the device: • **Managed—**Device is in a fully managed state. • **Partial Collection Failure—**Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the **Information** (i) icon to display additional information about the failure. • **Unreachable—**Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place. • **Wrong Credentials—**If device credentials are changed after adding the device to the inventory, this condition is noted. • **In Progress—**Inventory collection is occurring.

Device Inventory and Cisco ISE Authentication

After you provision a device, DNA Center authenticates the device with Cisco ISE. If Cisco ISE is not reachable (no RADIUS response), the device uses the local login credentials (what are the local login credentials?). If Cisco ISE is reachable but the device does not exist in Cisco ISE or its credentials do not match the credentials configured in DNA Center, the device does not fall back to use the local login. Instead, it goes into a partial collection state.

To avoid this situation:

- Make sure to add the credentials that you used for discovering the device to Cisco ISE.
- Do not configure device credentials that have fewer than 4 alphanumeric characters. Although devices may have credentials with fewer than 4 alphanumeric characters, Cisco ISE allows 4 alphanumeric characters as the minimum username and password length. If the device credentials have fewer than 4 characters, DNA Center cannot collect the device's inventory data, and the device goes into a partial collection state.
- Do not use credentials that have the same username but different passwords (cisco/cisco123 and cisco/pw123). WhileDNA Center allows the discovery of devices with the same username but different passwords, Cisco ISE does not allow this. If a duplicate username is used, DNA Center cannot authenticate the device and collect its inventory data, and the device goes into a partial collection state.

Device Inventory Tasks

You can perform several actions from the **Device Inventory** window. To display the action buttons, check a check box next to a device (or check the check box at the top of the list to select all devices).

Table 3: Device Inventory Buttons

Button	Action
Set Device Tags	Groups devices according to common attributes. For more information, see Add or Remove a Device Tag in Device Inventory, on page 14.
Delete	Deletes the selected devices from inventory. For more information, see Delete a Device, on page 15.
Update Credentials	Changes the credentials of the selected devices. In future discoveries, these credentials are used for the selected devices instead of the global or job-specific credentials. For more information, see Update Device Credentials, on page 15
Update Polling Time	Updates the polling interval of the selected devices. These device-specific settings override the global and job-specific settings for the selected devices. For more information, see Update Device Polling Interval, on page 19.

Button	Action
Resync (Resynchronize Devices)	Polls the selected devices for updated device information and status. For more information, see Resynchronize Device Information, on page 19.
Export	Saves the device inventory information as a CSV file. You provide a password to encrypt the CSV file. Users who want to import the file must enter this password to open the exported file. For more information, see Export Device Configurations, on page 21.
Import Device(s)	Updates the devices in inventory with the information from an imported file. Device synchronization is started. Access Points are ignored in the device import operation. DNA Center provides a sample template in the GUI.

Add a Device Manually

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Click **Add Device**.

Step 3 In the **Add Device** dialog box, enter the device's IP address in the **Device IP** field.

Step 4 In the **Compute Device** field, choose either **TRUE** or **FALSE**, as follows:

- If the device is a Network Functions Virtualization (NFV) or data center device, choose **TRUE** and go to the next step.
- If the device is not an NFV or data center device, choose **FALSE** and go to Step 6.

The default is **FALSE**.

Step 5 If you chose **TRUE** for the **Compute Device** field, configure the **HTTP(S)** fields and click **Add**.

Table 4: HTTPS Credentials

Field	Description
Username	Name used to authenticate the HTTPS connection.
Password	Password used to authenticate the HTTPS connection.

Field	Description
Port	Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

Step 6 In the **SNMP** area, choose the SNMP version from the **Version** drop-down list (**V2C** or **V3**).
If you chose **V2C**, configure the following fields:

Table 5: SNMP v2c Credentials

Field	Description
Read	• **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Read Community—**Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Write Community—**Write community string used to make changes to SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

If you chose **V3**, configure the following fields:

Table 6: SNMP v3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires, and whether the message should be authenticated. Select one of the following modes: • **noAuthNoPriv—**Provides authentication or encryption. • **AuthNoPriv—**Provides authentication but does not provide encryption. • **AuthPriv—**Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Select one of the following authentication types: • **SHA—**Authentication based on HMAC-SHA. • **MD5—**Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. Passwords (or passphrases) must be at least 8 characters in length. **Note** • For several Cisco Wireless Controllers (WLC), passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords results in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as a the authentication mode.) Select one of the following privacy types: • **DES—**DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • **AES128—**CBC mode AES for encryption. • **None—**No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long. **Note** • For several Cisco WLCs, passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the fields.

Table 7: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.

Field	Description
Timeout (in Seconds)	Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.

Step 8 Expand the **CLI** area, if it is not already expanded, and configure the following fields:

Table 8: CLI Credentials

Field	Description
Protocol	Network protocol that enables DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**. If you plan to configure the NETCONF port (see next step), you need to choose **SSH2** as the network protocol.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. For security reasons, enter the enable password again. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 9 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.
NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 10 Click **Add**.

Filter Devices

Note To remove or change the filters, click **Reset**.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Click **Filters**.
The following filters are displayed:

- **Device Name**
- **IP Address**
- **Last Inventory Collection Status**

Step 3 Enter the appropriate value in the selected filter field, for example, for the **Device Name** filter, enter the name of a device.
DNA Center presents you with auto-complete values as you enter values in the other fields. Choose one of the suggested values or finish entering the desired value.

You can also use a wildcard (asterisk) with these filters, for example, you can enter values with an asterisk at the beginning, end, or in the middle of a string value.

Step 4 Click the plus (+) icon to filter the information.
The data displayed in the **Devices** table is automatically updated according to your filter selection.

Note You can use several filter types and more than one value per filter.

Step 5 (Optional) If needed, add more filters.
To remove a filter, click the **x** icon next to the corresponding filter value.

Change Devices Layout View

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Click ⋮ and choose one of the following layout presets:

- **Status—**Displays general device status information, including **Up Time**, **Update Frequency**, and **Number of Updates**.
- **Hardware—**Displays hardware information, including **IOS/firmware**, **Serial Number**, and **Device Role**.
- **Tagging—**Displays tagging information, including **Device Role**, **Location**, and **Tag**.

Step 3 To customize your layout, select the columns that you want to display.
A blue check mark next to a column means that the column is displayed in the table.

Change Device Role (Device Inventory)

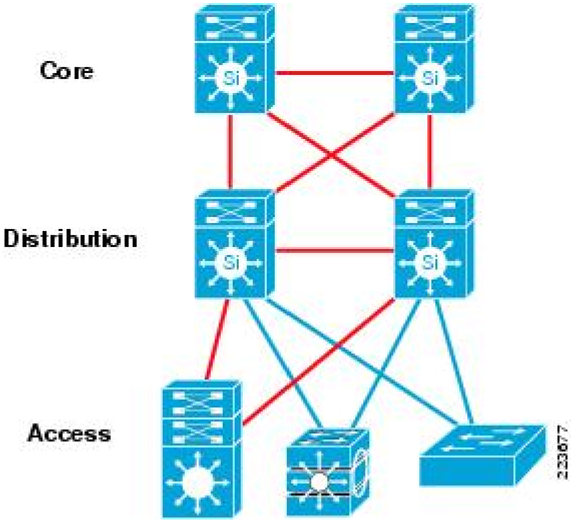
During the discovery process, DNA Center assigns a role to each of the discovered devices. Device roles are used to identify and group devices according to their responsibilities and placement in the network.

A device can have one of the following roles:

- **Unknown—**Device role is unknown.
- **Access—**Device is located in and performs the tasks required of the access layer, first tier, or edge of the network.
- **Border Router—**Device performs tasks required of a border router.
- **Distribution—**Device is located in and performs the tasks required of the distribution layer of the network.

- **Core—**Device is located in and performs the tasks required of the core of the network.

Figure 1: Device Roles and Network Locations



Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Locate the device whose role you want to change and choose a new role from the **Device Role** drop-down list.
Valid choices are **Unknown**, **Access**, **Core**, **Distribution**, or **Border Router**.

Add or Remove a Device Tag in Device Inventory

You can group devices according to common attributes by applying device tags. For example, you can apply device tags to group devices according to their platform ID or Cisco IOS release. A single device can have multiple device tags; similarly, a single device tag can be applied to multiple devices.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Check the check box next to the devices and click **Set Device Tags**.

Note For a single device, click the number displayed in the **Device Tag** column.

Step 3 Do one of the following tasks:

- To apply a device tag, from the **Available Tags** list, click the tags that you want to apply to the selected devices.

Note If the tag is not in the list, you can add a new tag by clicking +, entering a name for the tag, and clicking the check mark.

- To remove a device tag, from the **Applied Tags** list, click 🗑 next to the tag that you want to remove from the selected devices list.

Note The **Applied Tags** list is populated only if at least one of the selected devices has a tag applied to it.

Step 4 Click ✖ to close the dialog box.

Delete a Device

You can delete devices from the DNA Center database.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click the **Device Inventory** tool.

Step 2 Check the check box next to the device or devices that you want to delete.

Note You can select multiple devices by clicking additional check boxes, or you can select all devices by clicking the check box at the top of the list.

Step 3 Click **Delete**.

Update Device Credentials

You can update the discovery credentials of selected devices. The updated settings override the global and job-specific settings for the selected devices.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Select the devices that you want to update.

Step 3 Click **Update Credentials**.

Step 4 Click **OK** to confirm this action.

Step 5 From the **Update Credentials** dialog box, expand the **SNMP** area, if it is not already expanded.

Step 6 From the **Version** field, choose the SNMP version (**V2C** or **V3**).

Note Because both the SNMP and CLI credentials are updated together, we recommend that you provide both credentials. If you provide only SNMP credentials, DNA Center saves only the SNMP credentials, and the CLI credentials are not updated.

Step 7 Depending on the whether you choose **V2C** or **V3**, enter information in the remaining fields, which are described in the following tables.

Table 9: SNMP v2c Credentials

Field	Description
Read	• **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Read Community—**Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Write Community—**Write community string used to make changes to SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 10: SNMP v3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.

Field	Description
Mode	Security level that an SNMP message requires, and whether the message should be authenticated. Select one of the following modes: • **noAuthNoPriv—**Provides authentication or encryption. • **AuthNoPriv—**Provides authentication but does not provide encryption. • **AuthPriv—**Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Select one of the following authentication types: • **SHA—**Authentication based on HMAC-SHA. • **MD5—**Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. Passwords (or passphrases) must be at least 8 characters in length. **Note** • For several Cisco Wireless Controllers (WLC), passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords results in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as a the authentication mode.) Select one of the following privacy types: • **DES—**DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • **AES128—**CBC mode AES for encryption. • **None—**No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long. **Note** • For several Cisco WLCs, passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and complete the following fields:

Table 11: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.
Timeout (in Seconds)	Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.

Step 9 Expand the **CLI** area, if it is not already expanded, and complete the following fields:

Note Both the SNMP and CLI credentials are updated together, so you need to provide both credentials. If you provide only SNMP credentials, DNA Center saves only the SNMP credentials. The CLI credentials are not updated.

Table 12: CLI Credentials

Field	Description
Protocol	Network protocol that enables DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**. If you plan to configure the NETCONF port (see next step), you need to choose **SSH2** as the network protocol.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. For security reasons, enter the enable password again. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 10 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 11 Click **Update**.

Update Device Polling Interval

You can update the polling interval at the global level for all devices by choosing **Settings > Network Resync Interval** or at the device level for a specific device by choosing **Device Inventory**. When you set the polling interval using the **Network Resync Interval**, that value takes precedence over the **Device Inventory** polling interval value.

If you do not want a device to be polled, you can disable polling.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Select the devices that you want to update.

Step 3 Click **Update Polling Interval**.

Step 4 From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.

Step 5 In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24-hours).

Note The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, DNA Center continues to use the device-specific polling time.

Step 6 Click **Update**.

Resynchronize Device Information

You can select the devices to be polled immediately for updated device and status information, regardless of the polling interval that is set. A maximum of 40 devices can be resynchronized at the same time.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Select the devices that you want to gather information about.

Step 3 Click **Resync**.

Step 4 Confirm the resynchronization by clicking **OK**.

Use a CSV File to Import and Export Device Configurations

CSV File Import

If you want to use a CSV file to import your device configurations or sites from another source into DNA Center, you can download a sample template by choosing (from the DNA Center home page) **Device Inventory > Import Devices**. Click **Download** to download a sample CSV file template.

When you use a CSV file to import device or site configurations, the extent to which DNA Center can manage your devices, depends on the information you provide in the CSV file. If you do not provide values for CLI username, password, and enable password, DNA Center will have limited functionality and cannot modify device configurations, update device software images, and perform any other valuable functions.

You can specify the credential profile in the CSV file to apply the credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, then the manually entered credentials take higher priority and the device is manged based on a combination of manually entered credentials and credential profile. For example, if the CSV file contains a credential profile with SNMP and Telnet credentials in addition to manually entered SNMP credentials, then the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.

Note You must also provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 username and authorization password.

For partial inventory collection in DNA Center, you must provide the following values in the CSV file:

- – Device IP address
- – SNMP version
- – SNMP read-only community strings
- – SNMP write community strings
- – SNMP retry value
- – SNMP timeout value

For full inventory collection in DNA Center, you must provide the following values in the CSV file:

- Device IP address

- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value
- Protocol
- CLI username
- CLI password
- CLI enable password
- CLI timeout value

CSV File Export

DNA Center enables you to create a CSV file that contains all or selected devices in the device inventory. When you create this file, you must enter a password to protect the configuration data that the file will contain.

Import Device Configurations From a CSV File

You can import device configurations from a CSV file.

Procedure

Step 1 From the DNA Center **Home** page, click **Device Inventory**.

Step 2 Click **Import Device(s)** to import all of the devices from the CSV file into **Device Inventory**.

Step 3 Drag and drop the CSV file into the boxed area in the **Bulk Import** dialog box or click the dotted-line boxed area and browse to the CSV file.

Step 4 In the **Export Device** dialog box, enter a password that will be used to encrypt the exported CSV file. Users will need to supply this password to open the exported file.

Step 5 Click **Import**.

Export Device Configurations

When you export the device list to a file, all of the device configurations are exported into a CSV file. The file is then compressed and encrypted using a password that you set. The exported file includes device credentials but does not include credential profiles.

Caution Handle the CSV file with care because it lists all of the credentials for the exported devices. Ensure that only users with special privileges perform a device export.

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Click **Export All** to export all of the devices in the inventory or select the devices that you want to export and click **Export**.

Step 3 In the **Export Device** dialog box, enter a password that will be used to encrypt the exported CSV file.
You need to supply this password to open the exported file.

Step 4 Confirm the encryption password and click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.