Configure Site Network Settings

About Global Network Settings

You can create network settings that become the default for your entire network. There are two primary areas for defining settings within your network:

- **Global settings** affect your entire network and can include settings for servers (such as NTP, Syslog, SNMP Trap, Netflow Collector, etc.), IP address pools, and device credential profiles.
- **Site settings** override Global settings and can include settings for servers, IP address pools, and device credential profiles.

You can define the following global network settings by choosing **Design > Network Settings > Network**.

- Network servers such as AAA, DHCP, and DNS Servers—See Configure Global Network Servers, on page 9.
- Device credentials such as CLI, SNMP, and HTTP(S) credentials—See Configure CLI Credentials, on page 4, Configure SNMPv2c Credentials, on page 5, Configure SNMPv3 Credentials, on page 6, and Configure HTTPS Credentials, on page 8.
- IP address pools—See Configure IP Address Pools, on page 9.
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—See Configure Global Wireless Settings

About Device Credentials

Device credentials refer to the CLI, Simple Network Management Protocol (SNMP), and HTTPS credentials that are configured on network devices. DNA Center uses these credentials to discover the devices in your network. In DNA Center, you can specify the credentials that most of the devices use so that you do not have to enter them each time you run a discovery job. These credentials are called global device credentials. Specify them using the DNA Center GUI (**Design > Network Settings > Device Credentials**). After you set up these credentials, they are available for use in the **Discovery** tool.

CLI Credentials

You need to configure the CLI credentials of your network devices in DNA Center before you can run a Discovery job.

CLI credentials are used to discover and gather information about network devices. During the Discovery process, DNA Center logs into the network devices using their CLI usernames and passwords and runs **show** commands to gather device status and configuration information. DNA Center also runs **clear** commands and other commands that perform actions that are not saved in a device's configuration.

SNMPv2c Credentials

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language to monitor and manage network devices.

SNMP version 2 (SNMPv2c) is the community string-based administrative framework for SNMPv2. It does not provide authentication or encryption (noAuthNoPriv level of security). Instead, it uses a community string as a type of password that is typically provided in cleartext.

Note In DNA Center's implementation, only the username is provided in clear text. SNMP community strings are not provided in cleartext for security reasons.

You need to configure the SNMPv2c community string values before you can discover your network devices using the Discovery function. The SNMPv2c community string values that you configure must match the SNMPv2c values that have been configured on your network devices. You can configure up to five read community strings and five write community strings in DNA Center.

If you are using SNMPv2 in your network, specify both the Read Only (RO) and Read Write (RW) community string values to achieve the best outcome. If you cannot specify both, we recommend that you specify the RO value. If you do not specify the RO value, DNA Center attempts to discover devices using the default RO community string, *public*. If you specify only the RW value, Discovery uses the RW value as the RO value.

SNMPv3 Credentials

The SNMPv3 values that you configure to use Discovery must match the SNMPv3 values that have been configured on your network devices. You can configure up to five SNMPv3 values.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with in transit.
- Authentication—Determines if a message is from a valid source.
- Encryption—Scrambles a packet's contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and a user's role. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption
- AuthNoPriv—Security level that provides authentication but does not provide encryption
- AuthPriv—Security level that provides both authentication and encryption

The following table describes what the combinations of the SNMPv3 security models and levels mean:

Table 1: SNMPv3 Security Models and Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	User Name	No	Uses a username match for authentication.
AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA) or Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA) .
AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • CBC-DES • CBC-AES-128	Provides authentication based on HMAC-MD5 or HMAC-SHA. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.

HTTPS Credentials

Hyper-Text Transfer Protocol Secure (HTTPS) is a secure version of HTTP that is based on a special PKI certificate store. In DNA Center, HTTPS is used to discover Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) devices only.

Configure Global Device Credentials

Configure CLI Credentials

You can configure and save up to five global CLI credentials.

Before You Begin

You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *DNA Center Installation and Configuration Guide*.

Procedure

Step 1 From the DNA Center home page, choose **Design > Network Settings > Device Credentials**.

Step 2 In the **CLI Credentials** area, click **Add**.

Step 3 Enter information in the following fields:

Table 2: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
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.

Field	Description
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, enter the enable password again. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **OK**.

Configure SNMPv2c Credentials

If you use SNMPv2c credentials to monitor and manage your network devices, configure the SNMPv2c values to discover your devices.

Before You Begin

- You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *DNA Center Installation Guide*.
- You must have your network's SNMP information available for this procedure.
-

Procedure

Step 1 From the DNA Center home page, select **Design > Network Settings > Device Credentials**.

Step 2 In the **SNMP** credentials area, click **Add**.

Step 3 For the SNMP type, click **SNMP v2c** and enter the following information:

Table 3: 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.

Field	Description
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.

Step 4 Click **OK**.

Configure SNMPv3 Credentials

If you use SNMPv3 to monitor and manage your network devices, configure the SNMPv3 values to discover your network devices.

Before You Begin

- You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *DNA Center Installation Guide*.
- You must have your network's SNMP information available.
-

Procedure

Step 1 From the DNA Center home page, choose **Design > Network Settings > Device Credentials**.

Step 2 In the **SNMP** credentials area, click **Add**.

Step 3 For the SNMP type, click **SNMP v3** and enter the following information:

Table 4: 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 4 Click **OK**.

Configure HTTPS Credentials

Procedure

Step 1 From the DNA Center **Home** page, select **Design > Network Settings > Device Credentials**.

Step 2 In the **HTTPS Credentials** area, click **Add**.

Step 3 Enter the following information:

Table 5: SNMP v2c Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to five HTTPS read credentials. • **Name/Description—**Name or description of the HTTPS credentials that you are adding. • **Username—**Name used to authenticate the HTTPS connection. • **Password—**Password used to authenticate the HTTPS connection. • **Port—**Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	You can configure up to five HTTP write credentials. • **Name/Description—**Name or description of the HTTPS credentials that you are adding. • **Username—**Name used to authenticate the HTTPS connection. • **Password—**Password used to authenticate the HTTPS connection. • **Port—**Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **OK**.

Configure IP Address Pools

You can manually create IP address pools.

Procedure

Step 1 Choose **Design > Network Settings > IP Address Pools**.

Step 2 Click **Add** and complete the required fields.

Step 3 Click **Overlapping** to specify overlapping IP address pool groups to allow different address spaces and concurrently use the same IP addresses in different address spaces.

Step 4 Click **Save**.

Configure Global Network Servers

You can define global network servers that become the default for your entire network.

Note You can override global network settings on a site by defining site-specific settings.

Procedure

Step 1 Choose **Design > Network Settings > Network**. A list of default servers appears.

Step 2 Enter the required information for the servers listed, or click **Add Servers** to add an NTP, Syslog, SNMP Trap, or Netflow Collector server.

Note You must define a DHCP server in order to create IP address pools.

Step 3 Complete the required fields, then click **Save**.

Configure Cisco WLC-High Availability from Cisco DNAC

Cisco WLC High Availability (HA) can be configured through Cisco Digital Network Architecture (DNA) Center. In DNA Center Release 2.0, only the formation of WLC-HA is supported and breaking of HA and switch-over options are not supported.

Related Topics

- Prerequisites for Cisco WLC High Availability, on page 10
- Configuring Cisco WLC-HA from Cisco DNA Center, on page 10
- What Happens During or After the High Availability Process is Complete, on page 11
- Commands to Configure and Verify Cisco WLC- High Availability, on page 11

Prerequisites for Cisco WLC High Availability

- Discovery and Inventory of Cisco WLC-1 and WLC-2 (to be formed as High Availability through the management interface) should be successful. The devices should be in the managed state.
- The service ports and the management ports of Cisco WLC-1 and WLC-2 should be configured.
- Redundancy ports of Cisco WLC-1 and WLC-2 should be physically connected.
- The management address of Cisco WLC-1 and WLC-2 should be in the same subnet. Also, the redundancy management address of WLC-1 and WLC-2 should be in the same subnet.

Configuring Cisco WLC-HA from Cisco DNA Center

Procedure

Step 1 Choose **Provision** > **Devices**, and click WLC-1 (configuring this as primary).

Step 2 Click the **High Availability** tab.

Step 3 Select the Select Secondary WLC drop-down list and enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses.
Ensure that these IP addresses are the unused IP addresses.

Step 4 Click **Configure HA**.
The HA configuration is initiated at the background using the CLI commands. First, the primary WLC is configured. On success, the secondary WLC is configured. After the configuration is complete, both the WLCs will reboot. This process may take up to 2.5 minutes to complete.

Step 5 After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **In Progress**. When DNA Center finds the HA pairing successful, **Sync Status** becomes **Complete**.
This is triggered by the inventory poller or by manual re-sync. By now, the secondary WLC (WLC-2) gets deleted from DNA Center. This flow indicates the successful HA configuration in WLC.

Note There is no real-time data display for Redundancy Summary. During HA pairing, under **Device Inventory**, Cisco WLC shows "Synching" but under **Provision > WLC** shows "Sync Completed".

Note You must perform HA on WLC before adding WLC to connectivity domain. Also ensure that the **Sync status** is **Complete** before adding to connectivity domain.

What Happens During or After the High Availability Process is Complete

1. Cisco WLC-1 and WLC-2 are configured with redundancy management, redundancy units, and SSO. The WLCs reboot in order to negotiate their role as active or stand by. Configuration is synced from active to stand by.
2. On the Show Redundancy Summary page, you can see these configurations:
   - SSO is Enabled
   - WLC1 is Active state
   - WLC2 is Hot Stand By state
3. Active WLCs management port will be shared by both the WLCs and will be pointing to active. GUI, Telnet, and SSH on the stand by WLC will not work. You can use the console and service port interface to control the stand by WLC.

Commands to Configure and Verify Cisco WLC- High Availability

The following are the configuration commands sent to primary WLC:

- **config interface address redundancy-management 9.10.45.xx peer-redundancy-management 9.10.45.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

The following are the configuration commands sent to secondary WLC:

- **config interface address redundancy-management 9.10.45.yy peer-redundancy-management 9.10.45.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

The following are the commands to verify HA configurations from Cisco WLC:

- Use the **config redundancy mode sso** command to check the HA related details.
- Use the **show redundancy summary** command to check the configured interfaces.