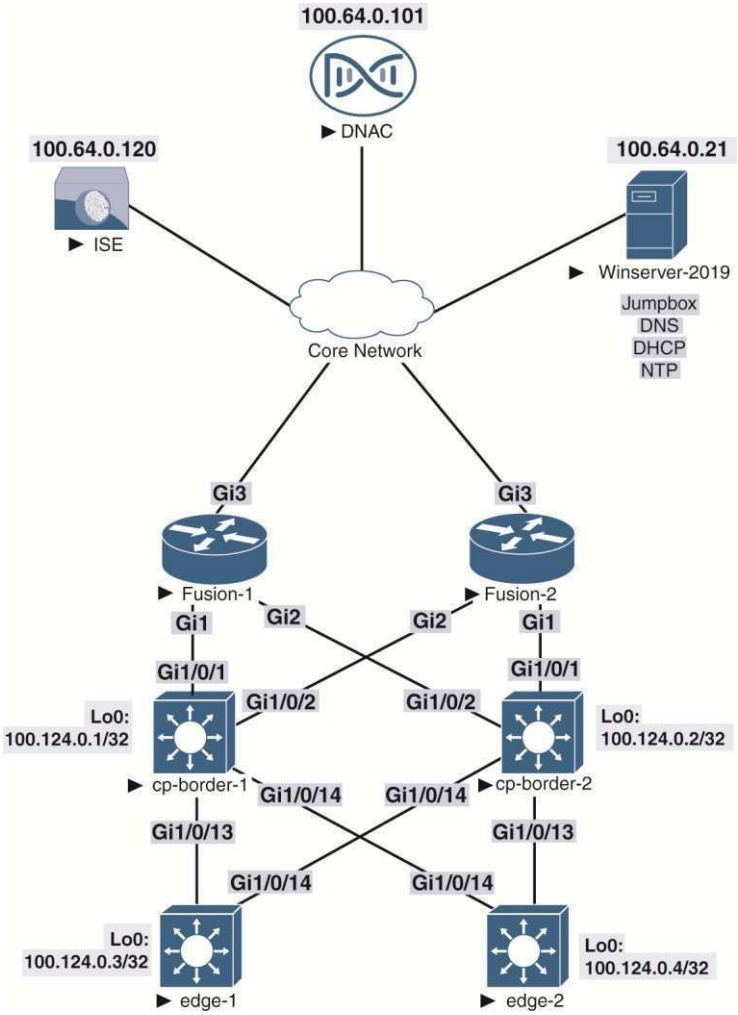
Chapter 11

CCIE
Enterprise Infrastructure
v1.1

SD-Access

The Introduction to SD-Access and DNA Center to enterprise network deployments gives the organization access to Cisco's latest features to automate common administrative tasks on security-focused programmable network infrastructures. This chapter will demonstrate the concept of a "Network Fabric" and the different node types that form it (Fabric Edge Nodes, Control Plane Nodes, Border Nodes). It demonstrates the roles of LISP in the Control Plane and VXLAN in the Data Plane for SD-Access Solutions and how DNA Center uses them to automate security and network access.

The following topology will be used for all the SDA labs:

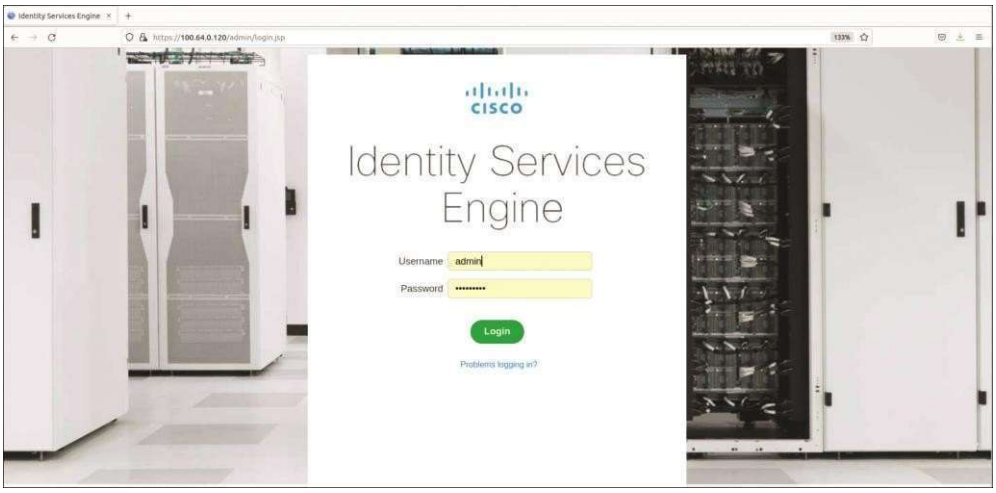


Lab 1: Configuring the SDA Policy Engine

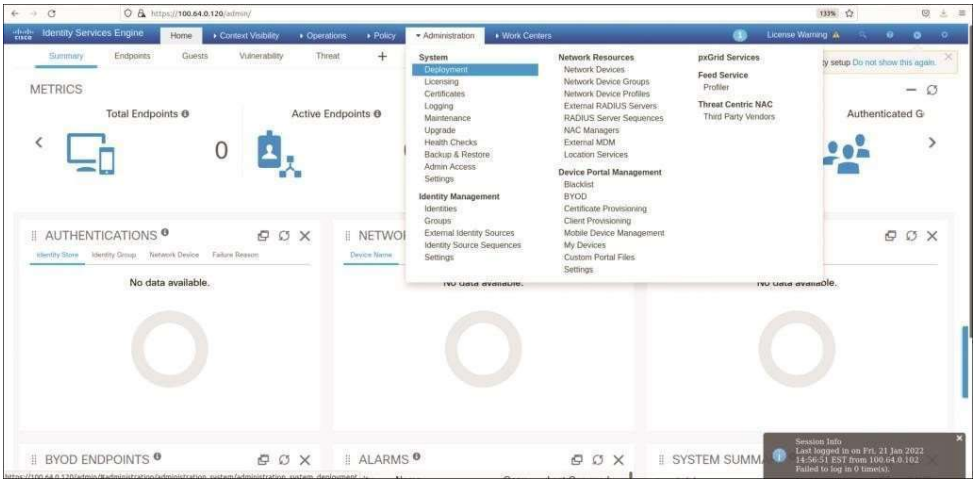
Task 1: ISE Integration with DNA Center

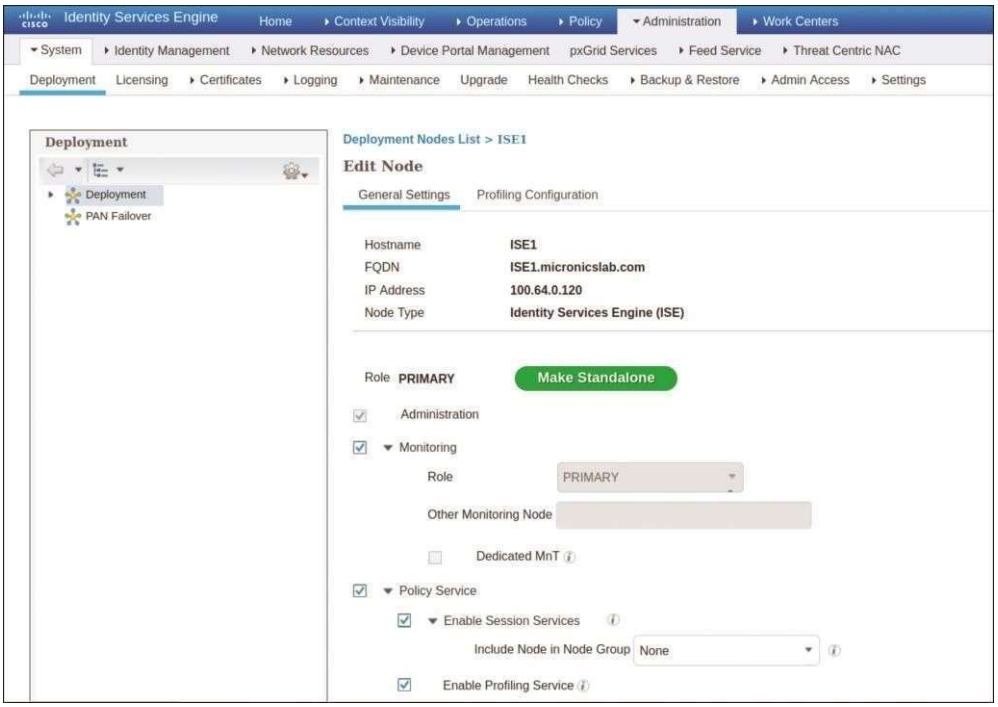
Setup the ISE for the first time and connect to ISE by using a browser by navigating to https://ise-ip. The IP address of ISE is 100.64.0.120. Use the following

Note: for this section, you can assign any IP in your lab for the above lab, and you need to install Cisco ISE in your eve-ng

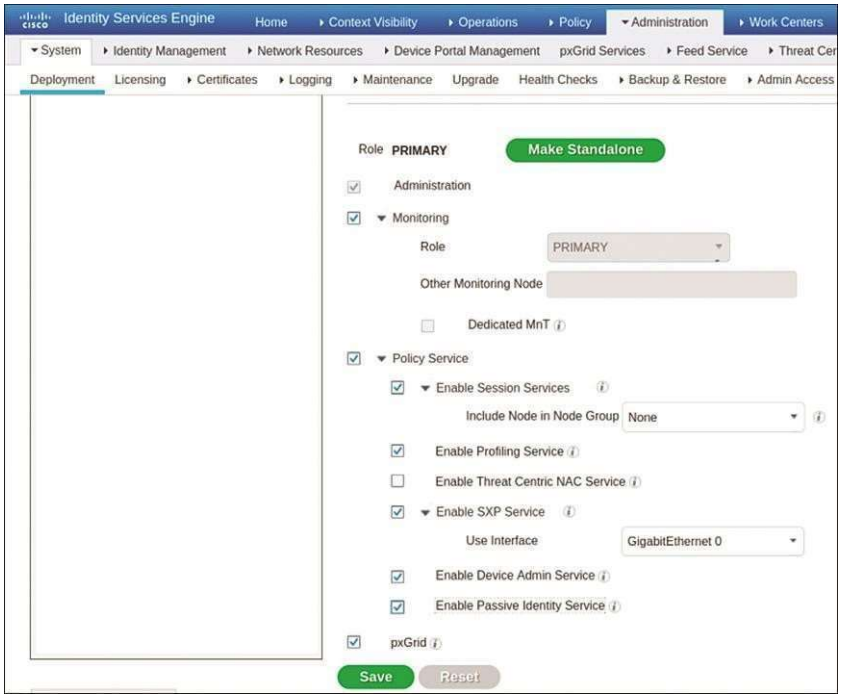


Navigate to **Administration > System > Deployment** and then click **OK** when you see the informational message shown below:





Enable the services SXP Service, Device Admin Service, Passive Identity Service, and pxGrid, as shown below, and click **Save.**



Navigateto **Administration>pxGrid Services** andcheckthe bannerinthelowerhalf of the screen. You should see “connected via XMPP” followed bythe FQDN of ISE, as shown on the next page. Make note of the FQDN, which you will need later. Keep in mind that this bannermightbered incolor initially because pxGrid services take some timeto initialize. You can

check the status of the services by logging in to ISE via the CLI and

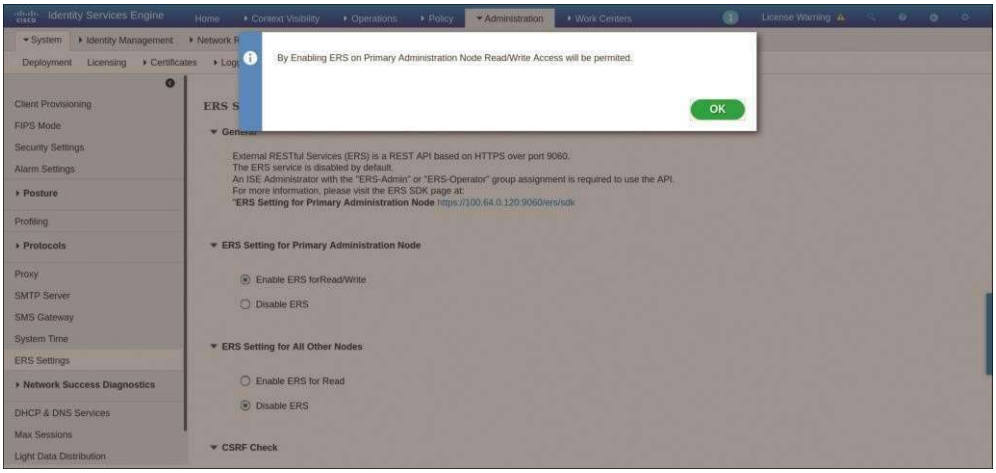
typing the command **show application status ise.**

```
Connected via XMPP ISE1.micronicslab.com
```

You should see output like the following:

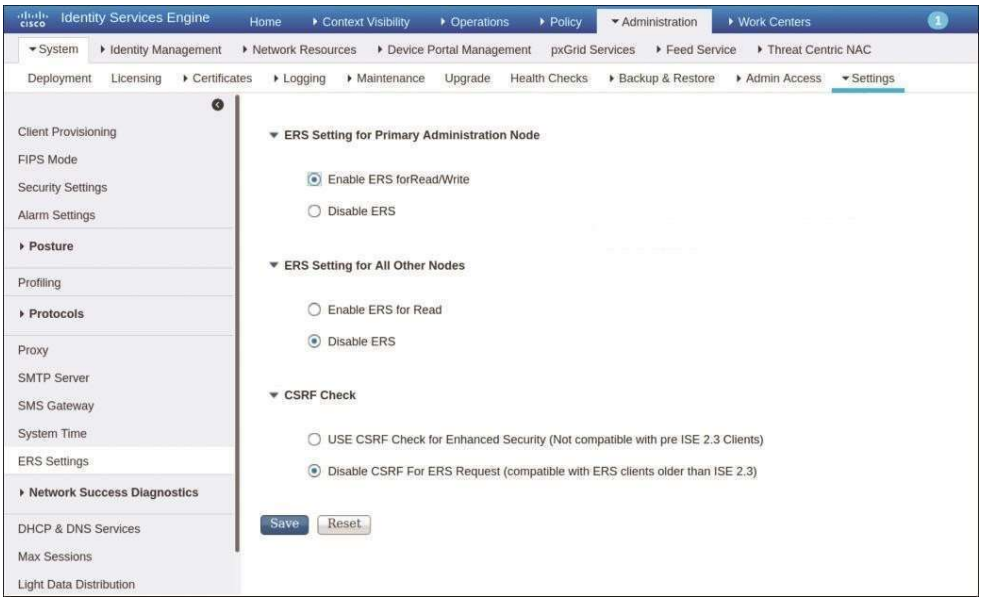
```
ise01/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          5235
Database Server                        running          138 PROCESSES
Application Server                     running          13618
Profiler Database                      running          8083
ISE Indexing Engine                    running          15878
AD Connector                           running          17756
M&T Session Database                   running          7892
M&T Log Processor                      running          13816
Certificate Authority Service          running          17042
EST Service                            running          29564
SXP Engine Service                     running          17589
Docker Daemon                          running          9407
TC-NAC Service                         disabled

Wifi Setup Helper Container            disabled
pxGrid Infrastructure Service          running          30552
pxGrid Publisher Subscriber Service    running          30708
pxGrid Connection Manager              running          30655
pxGrid Controller                      running          30776
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
```

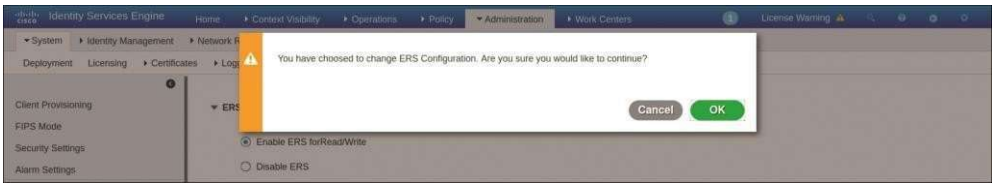
Navigate to **Administration > System > Settings > ERS Settings.** Then, under ERS Setting for Primary Administration Node, select **Enable ERS for Read/Write** and click **OK** in any dialog box that appears.



Under ERS Setting for All Other Nodes, select Enable ERS for Read, and under CRSF Check, select **Disable CSRF for ERS Request**, and then click **Save.**

Click **OK** in any additional dialog boxes that appear.

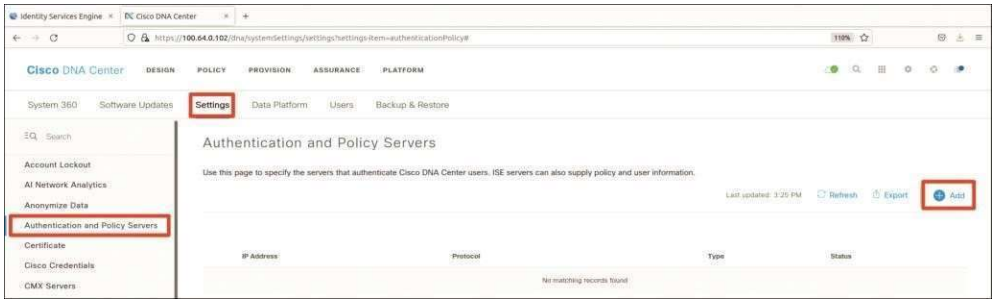

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Health Checks
Backup & Restore
Admin Access
Settings
Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
Posture
Profiling
Protocols
Proxy
SMTP Server
SMS Gateway
System Time
ERS Settings
Network Success Diagnostics
DHCP & DNS Services
Max Sessions
Light Data Distribution
ERS Setting for Primary Administration Node
Enable ERS forRead/Write
Disable ERS
ERS Setting for All Other Nodes
Enable ERS for Read
Disable ERS
CSRF Check
USE CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)
Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)
Save
Reset



Task 2: Finalize the Integration on DNA Center

Log in to the DNA Center web interface (https://100.64.0.101), at the top-right corner select the gear icon, and select **System Settings.** Use the provided credentials.

Navigate to **Settings > Authentication and Policy Servers** and then click **Add**:

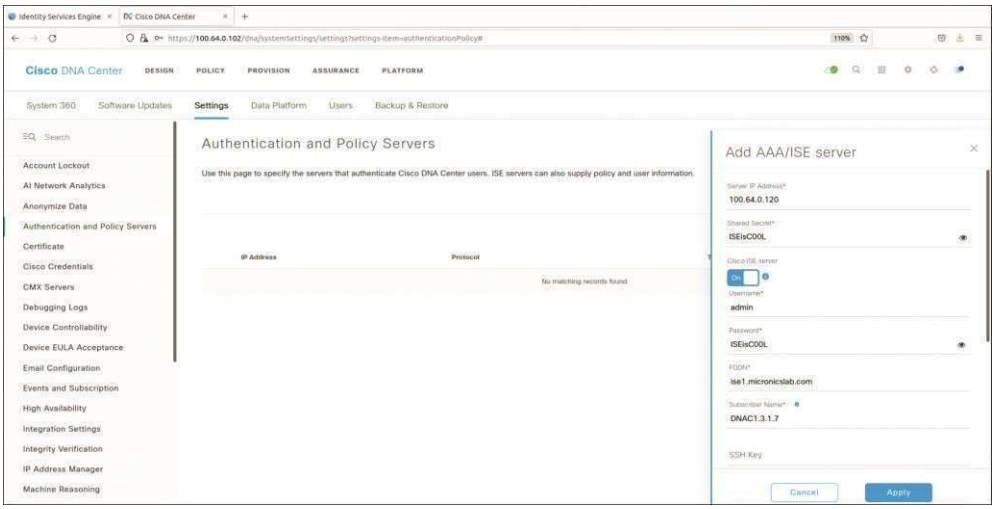


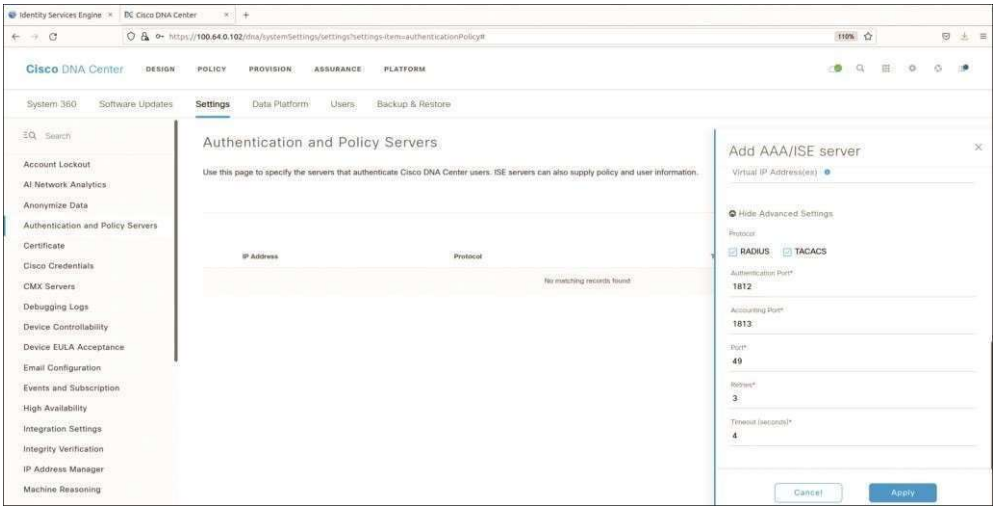
In the Add AAA/ISE Server display shown below, enter the ISE node (Primary PAN) IP address alongwith the details shown below:

Server IP Address	100.64.0.120
Shared Secret	ISEisC00L
ISE Selector	Toggle it to the on position
ISE Username	admin
ISE Password	-
ISE FQDN	Ise1.micronicslab.com (or IP)
Subscriber Name	DNAC1.3.1.7 (or above
SSH Key	<Leave Blank>
View Advanced Settings	Check TACACS and RADIUS

Note:

For this lab you will be using TACACS for network authentication and RADIUS for client authentication.

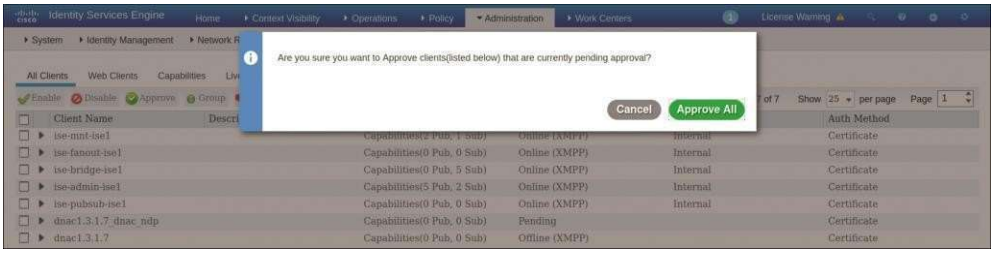




Click **Apply.**

Log in to ISE and navigate to **Administration > pxGrid Services.** The client named dnac1.3.1.7_dnac_ndp is now showing **Pending** in the Status column.

Choose **Total Pending Approval (1)**, click **Approve All**, and click **Approve All** again to confirm.

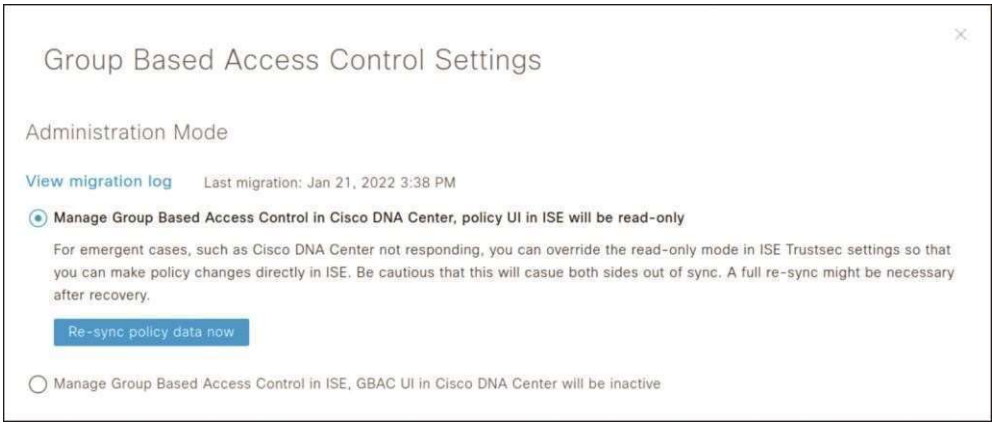


A success message appears.

If ISE is integrated with DNA Center after scalable groups are already created in ISE, in addition to the default groups, any existing ISE groups will also be visible. You can see these entries by logging in to DNA Center and navigating to **Policy > Group-Based Access Control > Scalable Groups**, as shown below:

For this exercise, you will use DNA Center to implement group-based access control. Click **Start Migration**, observe the warning message, shown below, and click **Yes.**

When the process is complete you will see the following success message.



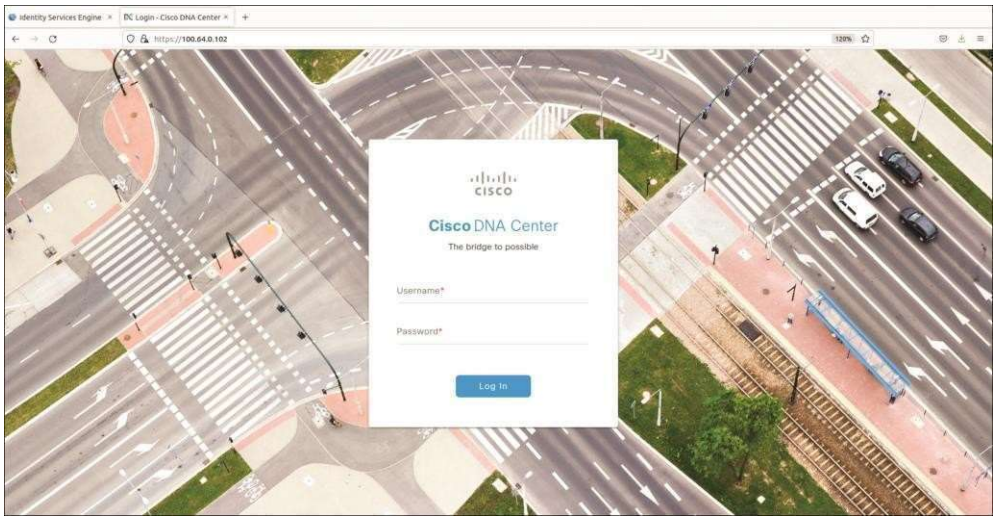
You should now see some additional Scalable Groups added (ACCT, HR, Campus Quarantine).

Lab 2: SDA Design

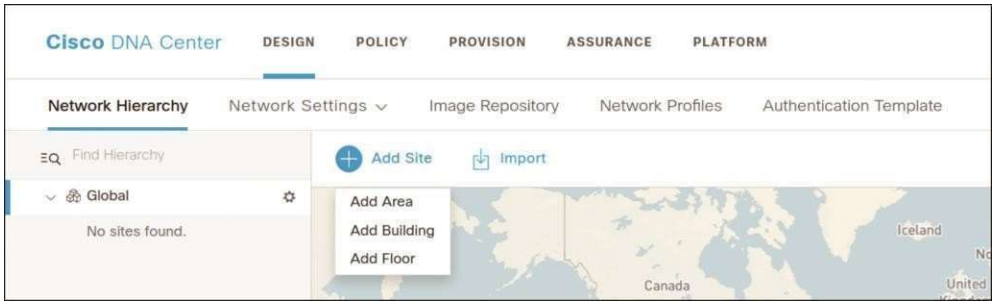
Task 1: Design the Network Hierarchy

Log in to ISE by using a browser to navigate to the IP address 100.64.0.120. Use the provided credentials.

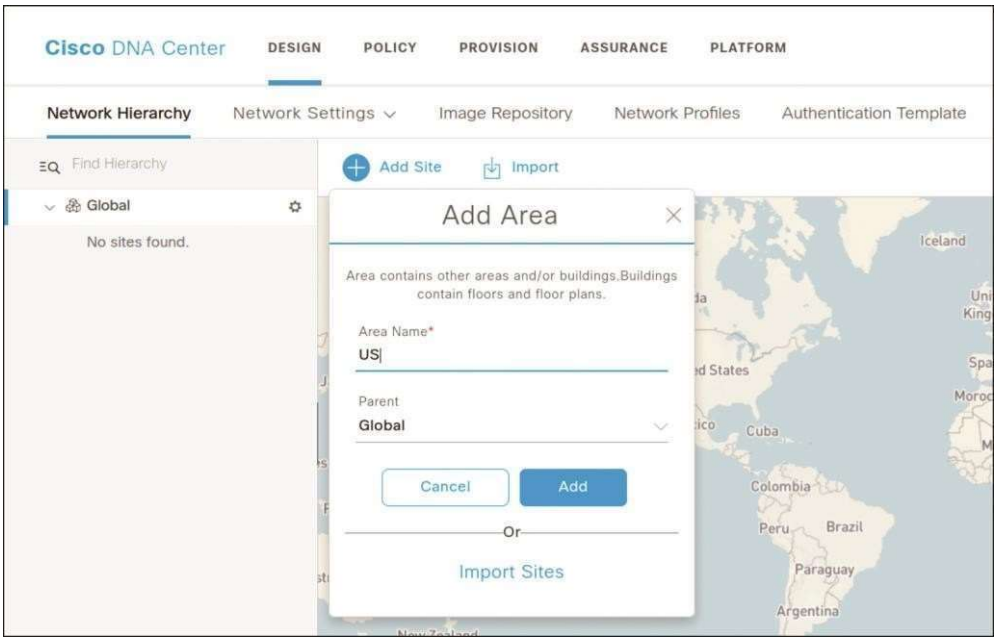
Log in to DNA Center by using a browser to navigate to https://100.64.0.101. Use the provided credentials



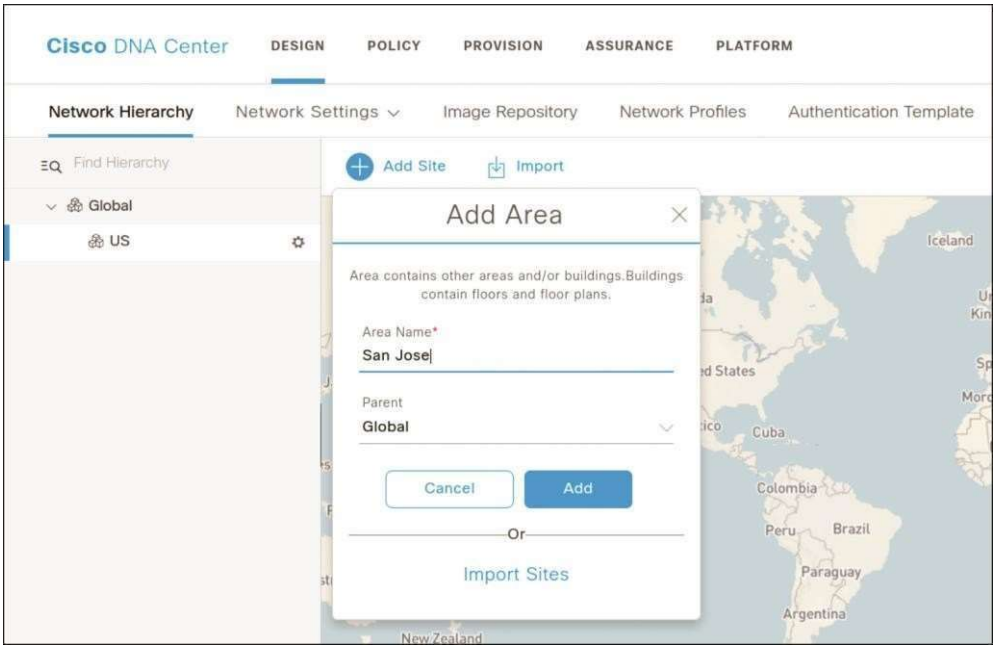
In DNA Center, go to **DESIGN > Network Hierarchy**, click **Add Site**, and select **Add Area**, as shown below:



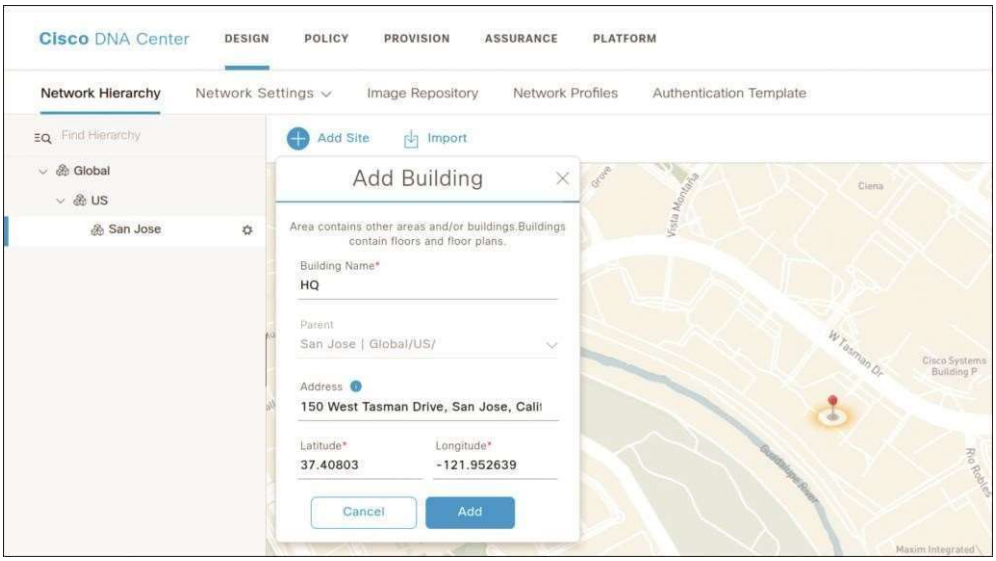
Enter **US** for the area name and click **Add**:



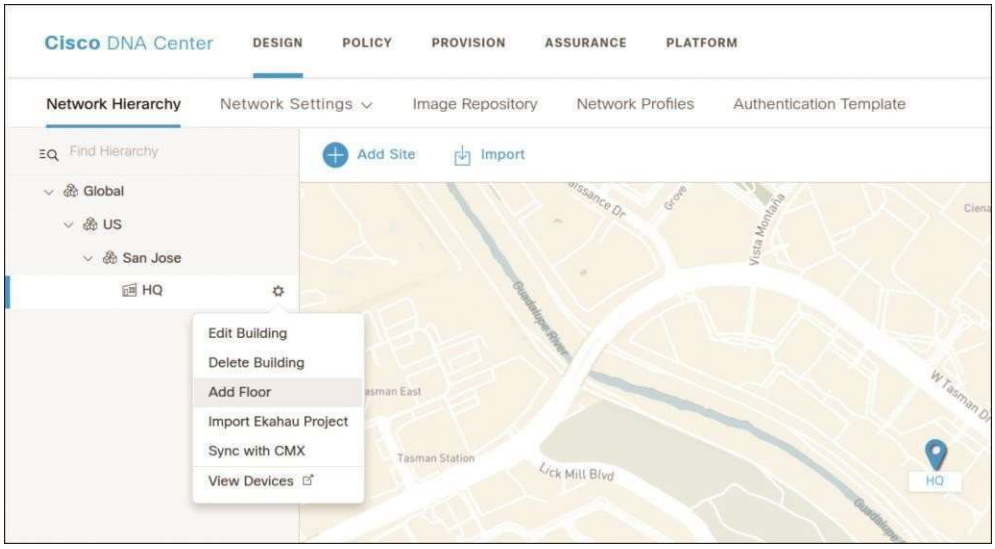
Click the cog wheel next to US in the navigation pane and choose **Add Area**. In the Add Area window, as shown below, enter **San Jose** for the area name and click **Add.**



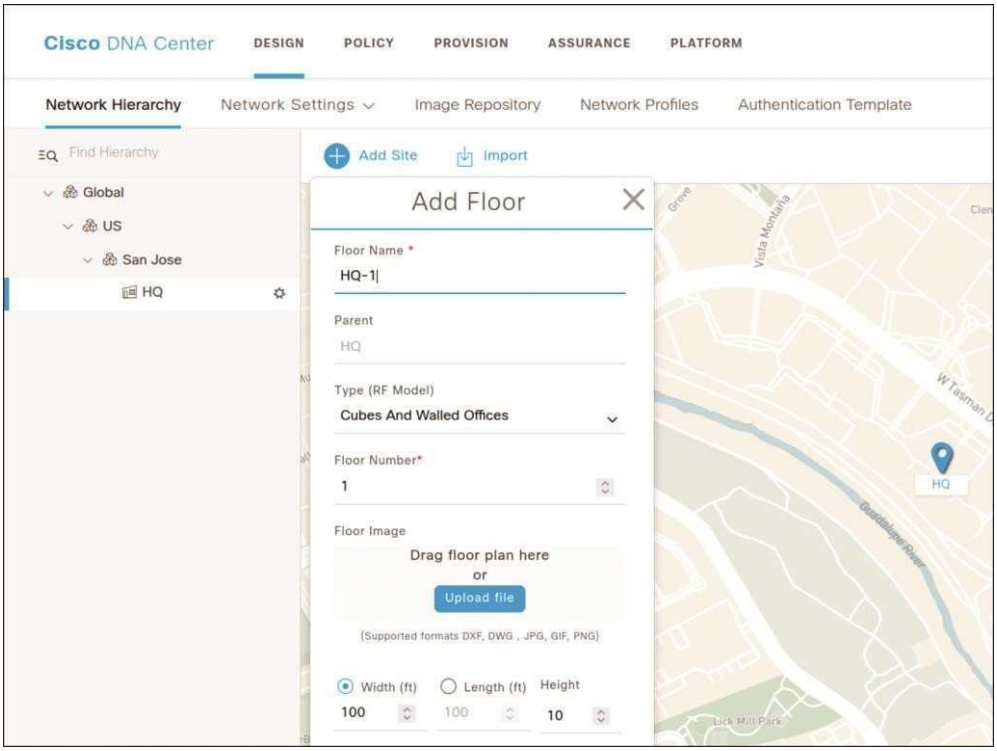
To add a building, select the cog wheel next to **San Jose** in the navigation pane and click **Add Building.** Enter the building name **HQ** and begin to enter the street address shown on the next page. Click on the correct option from among the street address recommendations that appear to autopopulate the Latitude and Longitude fields. Click **Add** when you're done with this.



With the building now defined, select **HQ** in the navigation pane, click the gear icon, and select **Add Floor**, as shown below:



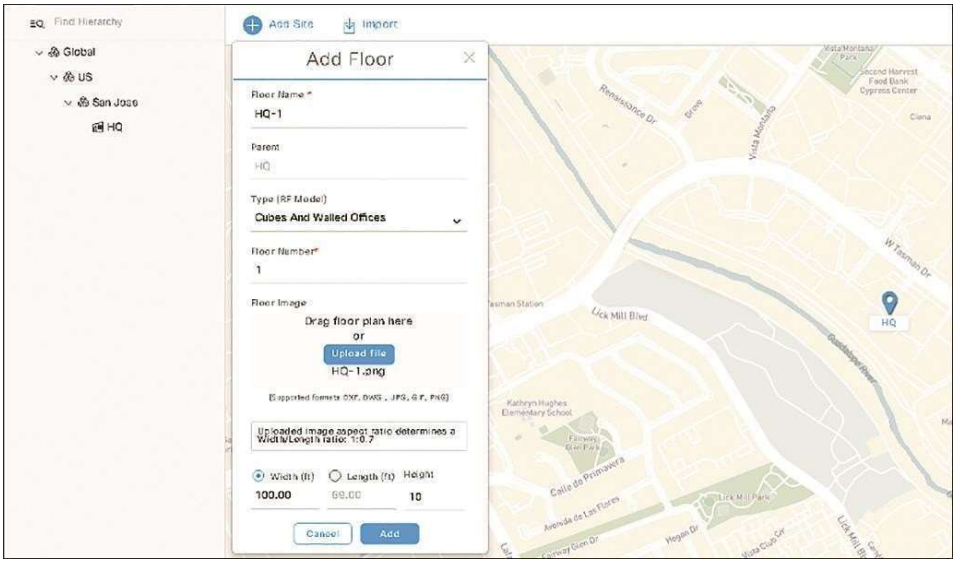
In the Add Floor window, enter **HQ-1** as the floor name and click **Upload File.**

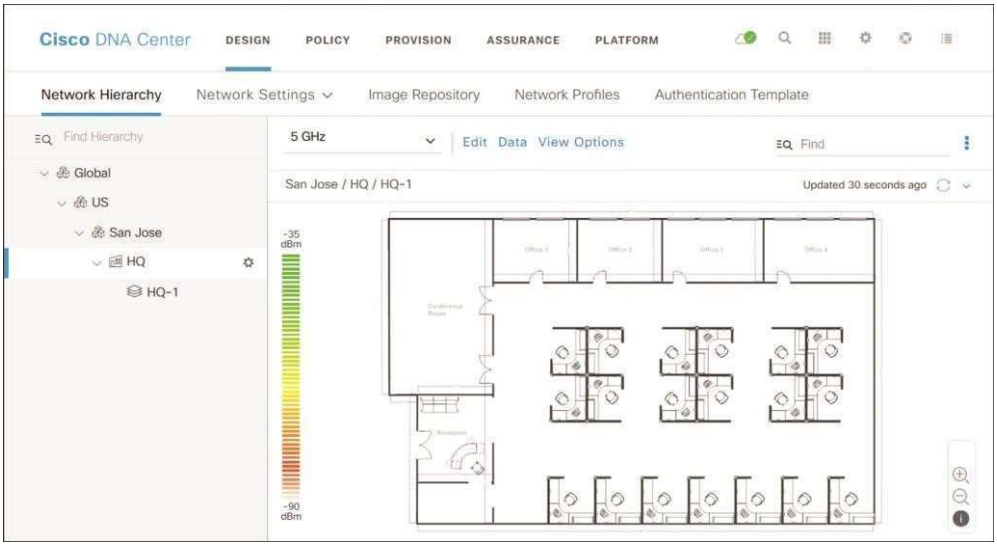


Note:

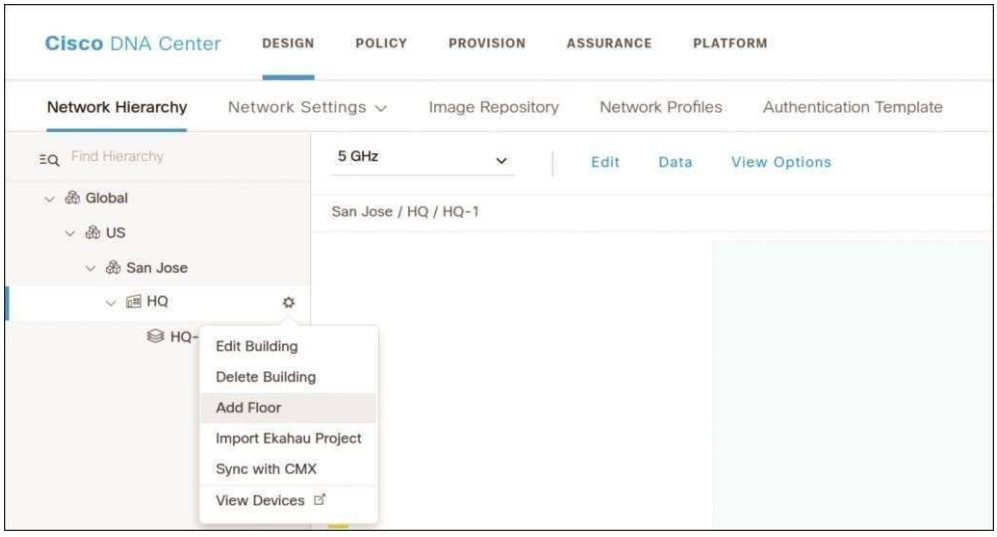
You should have floor plans and other files in the **Downloads folder.** Open it and select the **Floor Plan** folder. Look for **HQ-1.png** in this the folder and click **Open** to upload it.

DNA Center presents the floor plan file, as shown below. Click **Add** to create the floor.

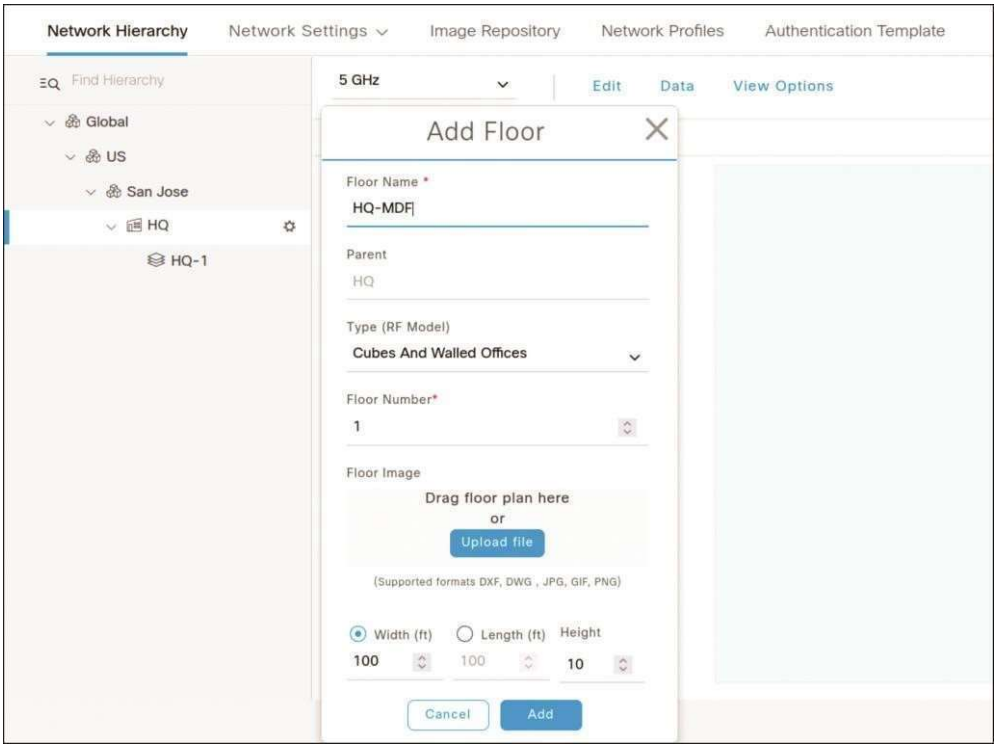




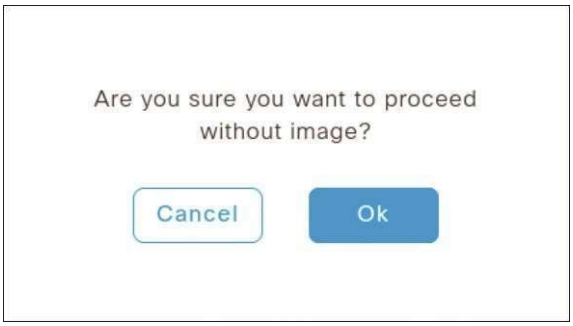
Return to **HQ** in the navigation pane, click the gear icon, and select **Add Floor** again to create another floor.



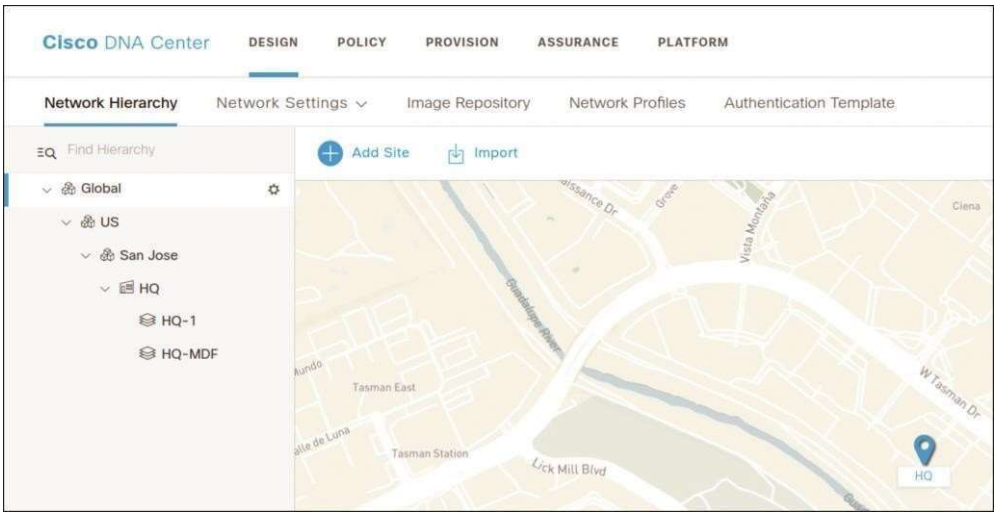
Name the new floor **HQ-MDF** and click **Add.** (You do not need to upload a floor plan in this case.)



Click **OK** to acknowledge the warning message and proceed without a floor plan for this floor.

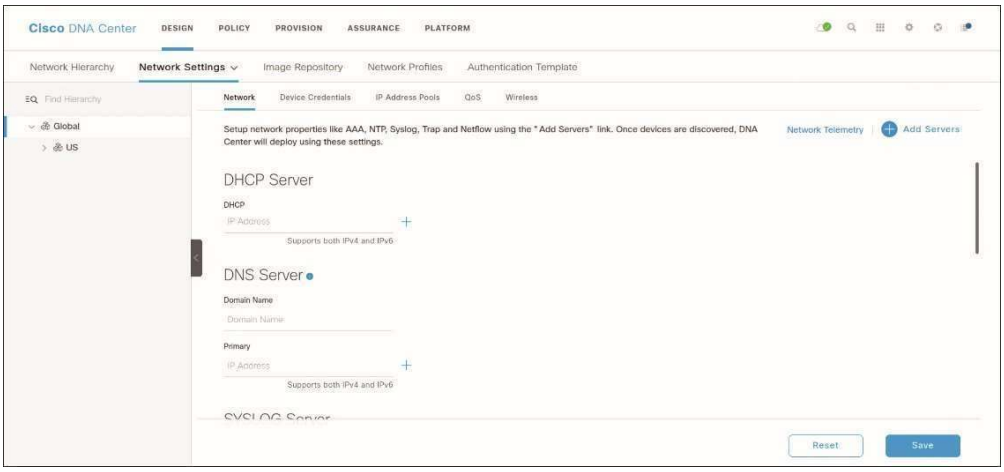


At this point, the building and floors necessary for this lab have been created. Observe the hierarchy you have built in the navigation pane shown on the next page:

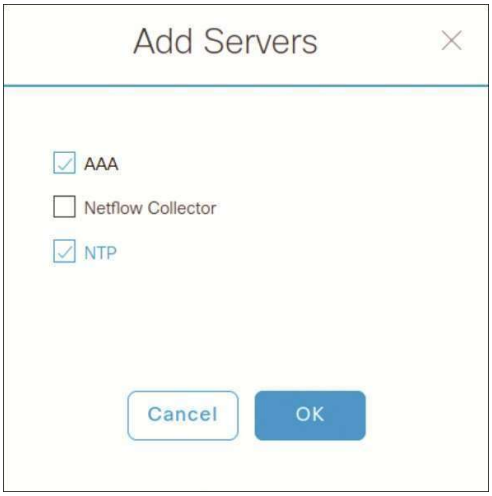


Task 2: Configure Common Network Settings

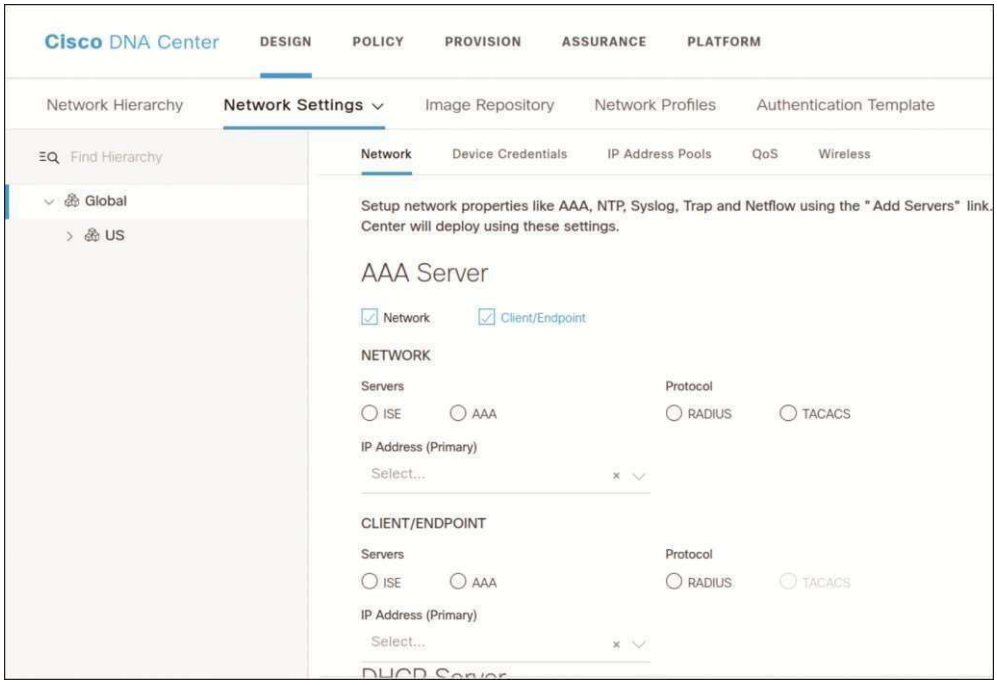
In DNA Center, navigate to **DESIGN > Network Settings > Network**, as shown below.



Ensure that **Global** is selected in the navigation pane and click **Add Servers.** Check the **AAA** and for **NTP** boxes and click **OK**:

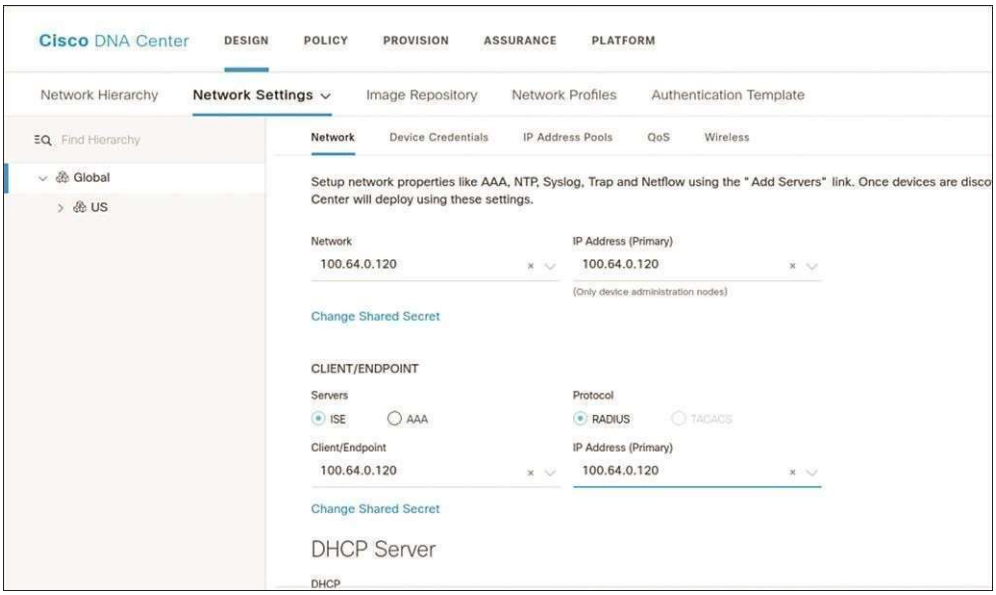


Notice that the AAA Server section is present. If you scroll to the bottom of the page, you also see an NTP section. Check the **Network** and **Client/Endpoint** boxes under AAA Server to reveal more options, as shown below.



As shown on the next page, in the Network section, select the ISE server **100.64.0.120** under both Network and IP Address (Primary).

In the CLIENT/ENDPOINT section, select the **ISE** radio button under Servers and the **RADIUS** radio button under Protocol.



Set the DHCP server to **100.64.0.2**, as shown below, and carefully enter the domain name **micronics.com** and the internal DNS server **100.64.0.2.**

Under NTP Server, enter **100.64.0.2** as the time source. Keep in mind that this is the CSR in the cloud that is providing time for the devices in the setup.

With all the Network Settings input at the Global Level, as shown below, click **Save.**

Confirmation messages like the ones on the next page appear briefly at the bottom right of the screen: