

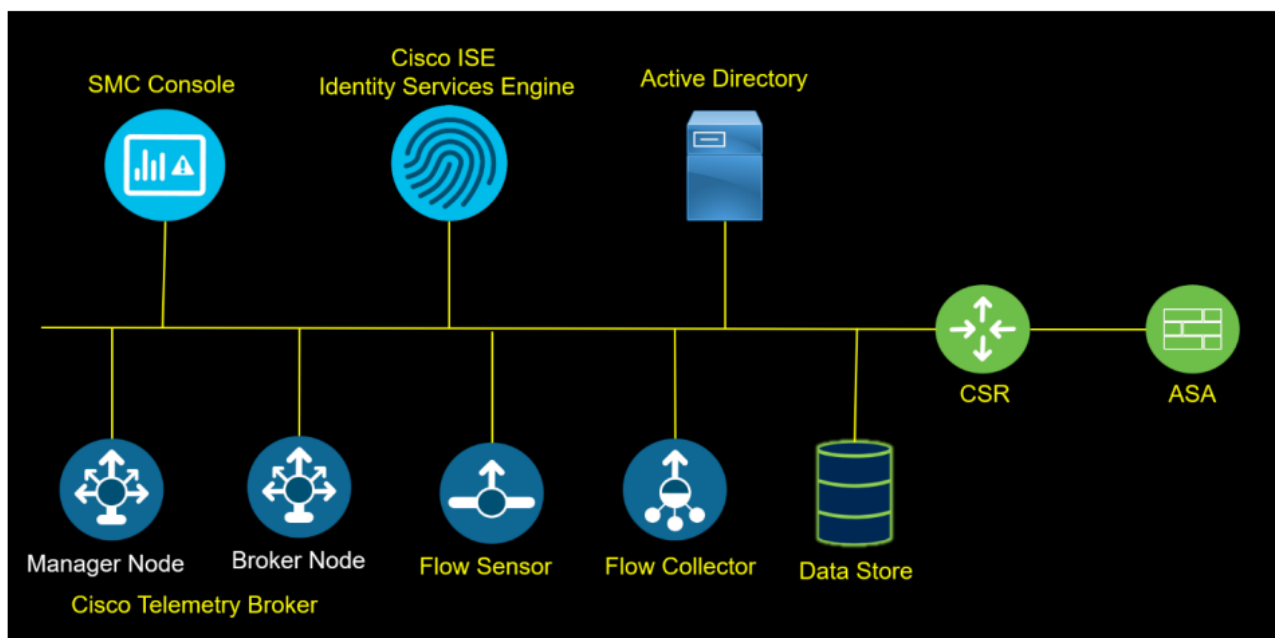


Contents [[hide](#)]

- 1 [CISCO Secure Network Analytics Deployment](#)
- 2 [Product Information](#)
- 3 [Installation of SMC](#)
- 4 [Installation of Datastore Node](#)
- 5 [Installation of Flow Collector](#)
- 6 [Installation of Flow Sensor](#)
- 7 [ISE Authorization Policies](#)
- 8 [FAQ](#)
- 9 [Documents / Resources](#)
 - 9.1 [References](#)



CISCO Secure Network Analytics Deployment



Product Information

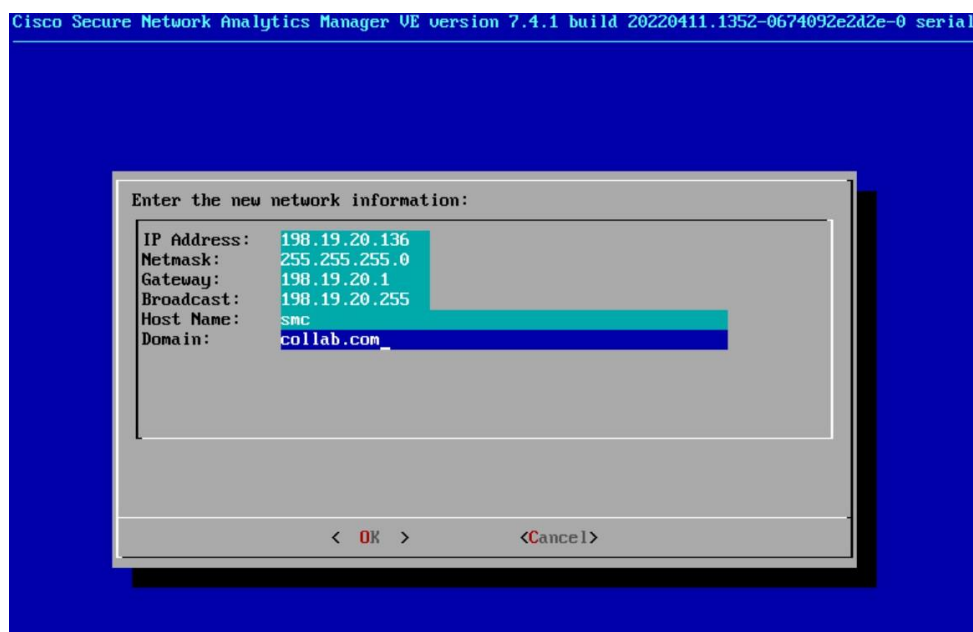
Specifications:

- Product Name: Cisco Secure Network Analytics Deployment
- Integration: Cisco ISE Integration for ANC

Cisco Secure Network Analytics Deployment and Cisco ISE Integration for ANC

Installation of SMC

Log in to the console, type the command SystemConfig. Enter the network configuration for the appliance.



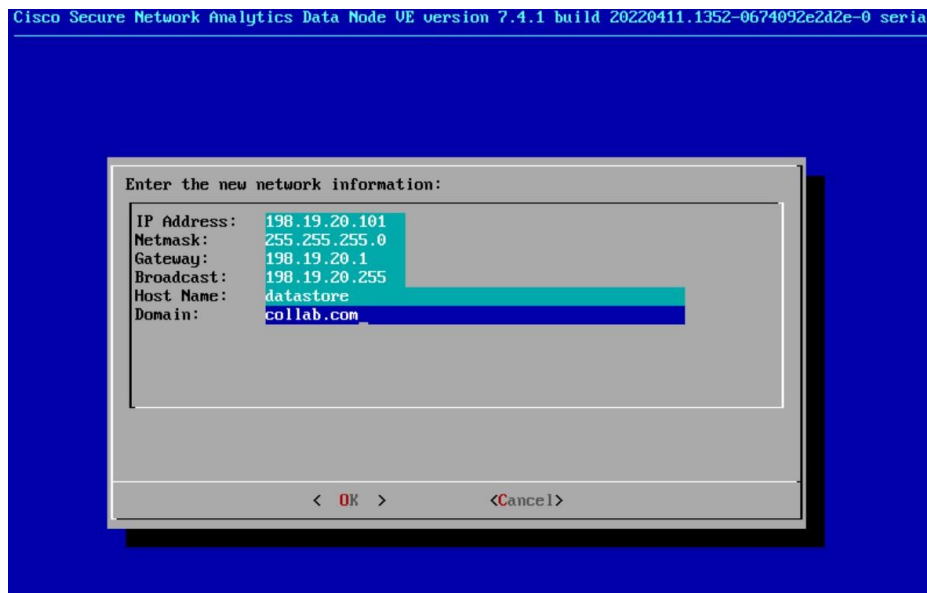
You have completed First Time Setup. Your appliance is ready to reboot. Reboot takes approximately 5-15 minutes to complete, depending on your appliance model. Select OK to save your configuration and reboot your appliance.

< OK >

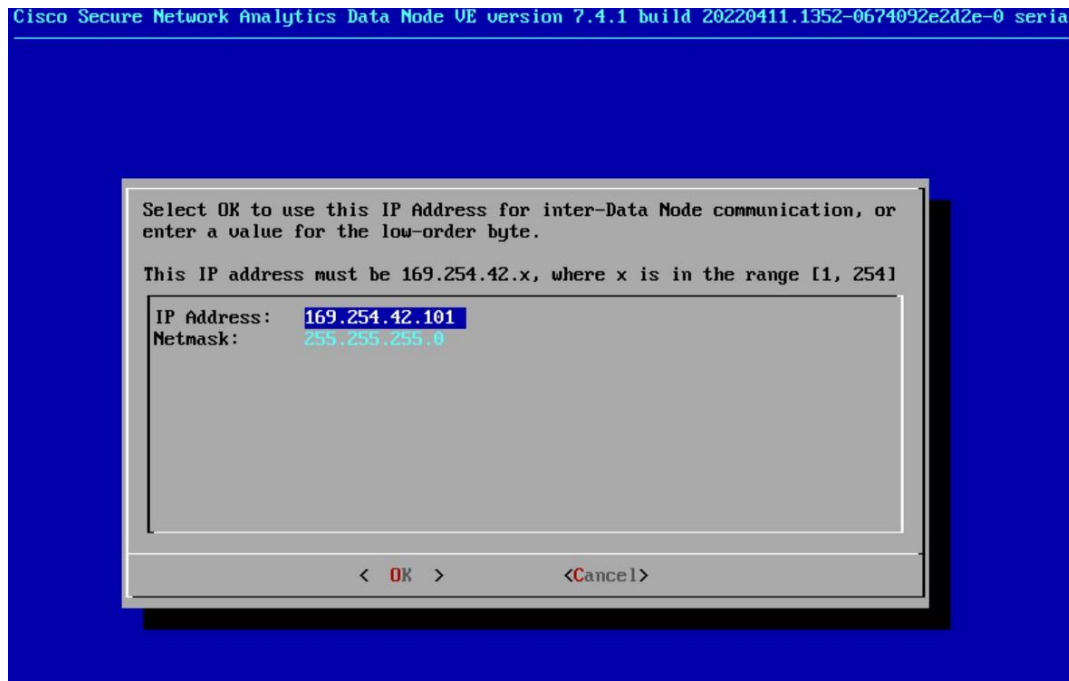
```
OK | Stopped Vertica Monitoring Service.
OK | Stopped irqbalance daemon.
OK | Removed slice system-getty.slice.
OK | Stopped LSB: Initialize EDAC.
OK | Stopped target System Time Synchronized.
OK | Stopped LSB: Start some power management scripts.
OK | Stopped LVM event activation on device 8:4.
OK | Removed slice system-lvm2\x2dpuscan.slice.
OK | Stopped LSB: Start pdnsd.
OK | Stopped Session 14 of user root.
    Stopping User Manager for UID 0...
    Stopping Login Service...
OK | Unmounted Persistent Journal Storage.
OK | Stopped User Manager for UID 0.
    Stopping User Runtime Directory /run/user/0...
OK | Unmounted /run/user/0.
OK | Stopped Availability of block devices.
OK | Stopped User Runtime Directory /run/user/0.
OK | Removed slice User Slice of UID 0.
    Stopping D-Bus System Message Bus...
    Stopping Permit User Sessions...
OK | Stopped LSB: set CPUFreq kernel parameters.
```

Installation of Datastore Node

Log in to the console, type the command `SystemConfig`. Enter the network configuration for the appliance.

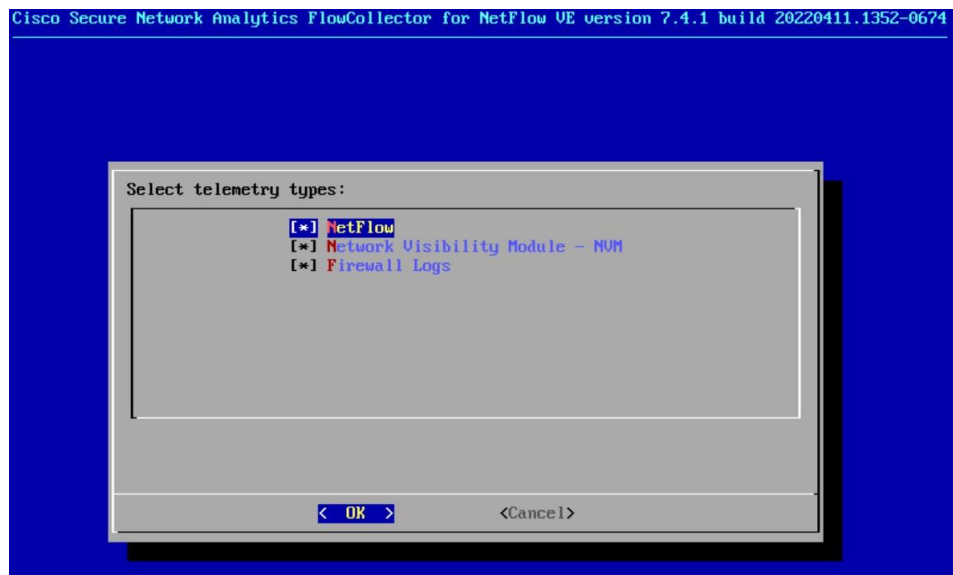


We have configured the management interface, the following is a second network interface for the inter-Data Node communication (communication with other data nodes).



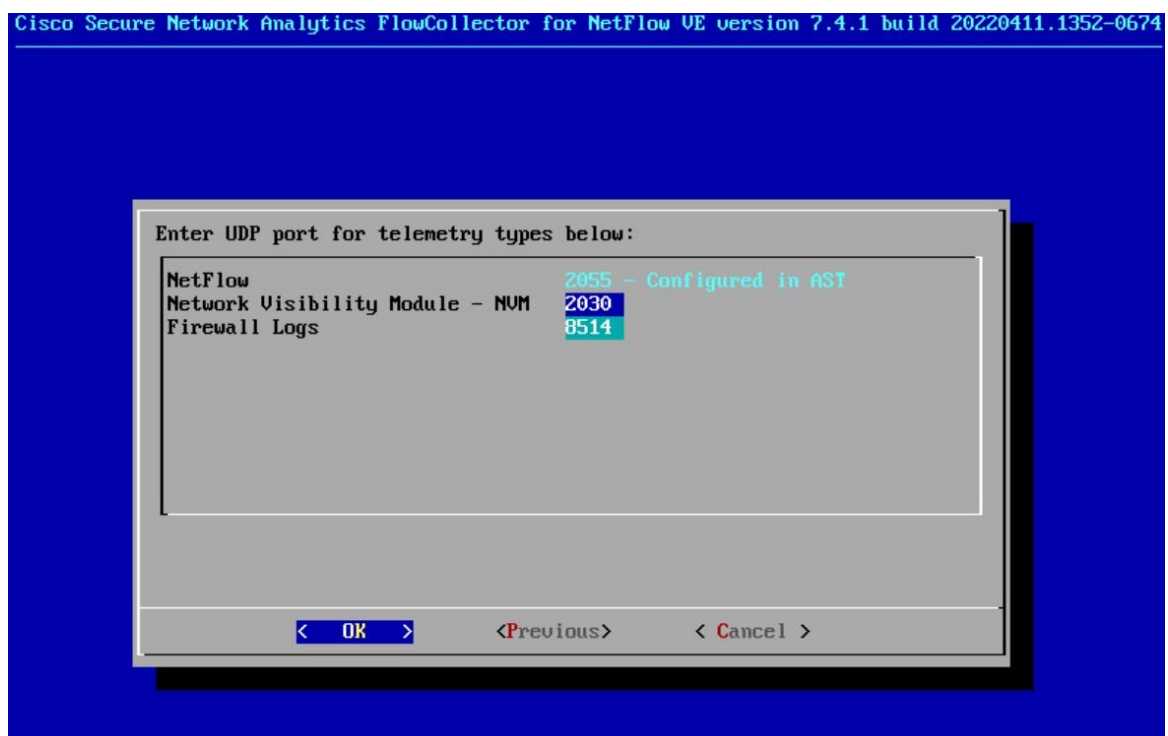
Installation of Flow Collector

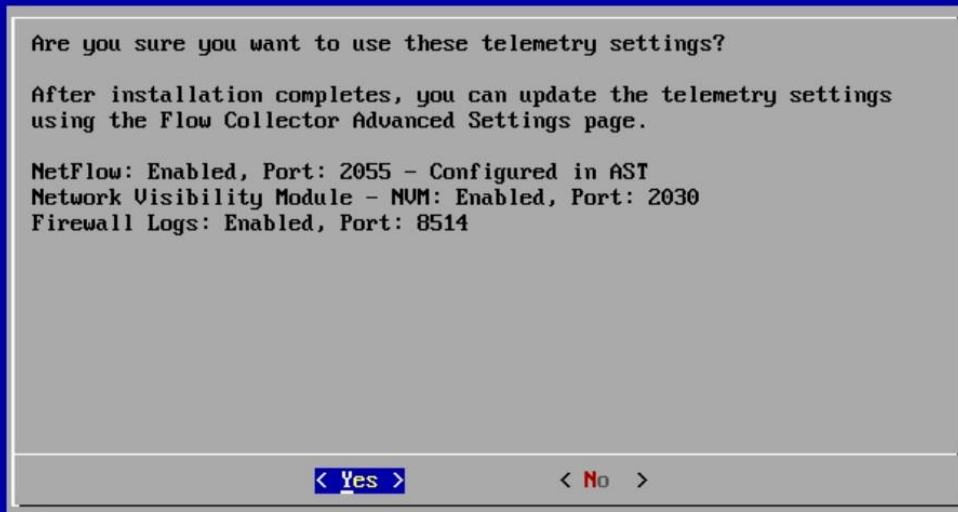
Log in to the console, type the command `SystemConfig`. Ensure that all telemetry options are selected.



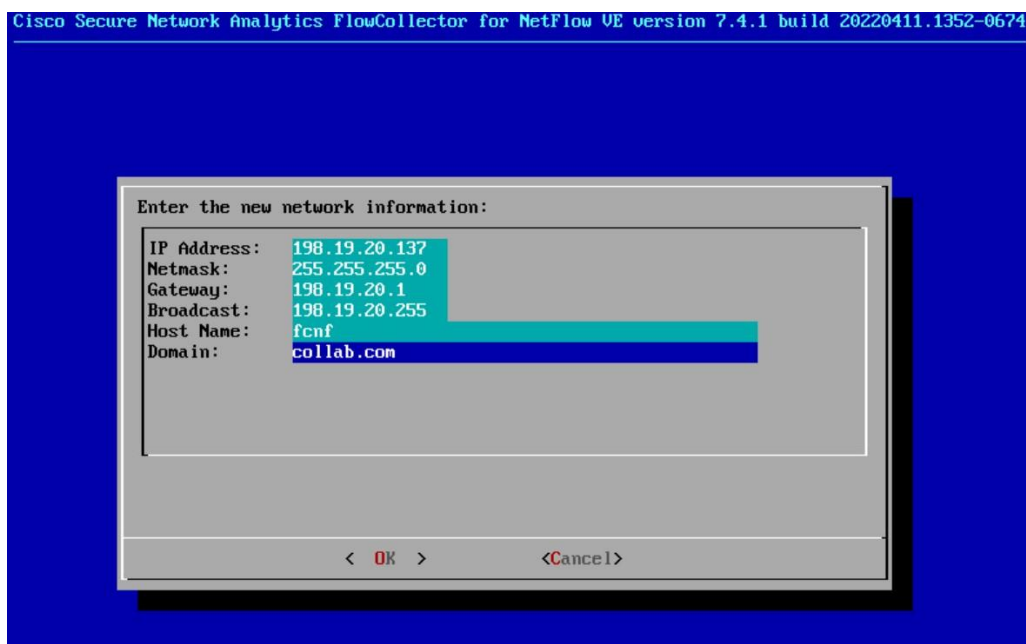
Configure the ports for the telemetry.

- Netflow: 2055
- Network Visibility Module: 2030
- Firewall Logs: 8514



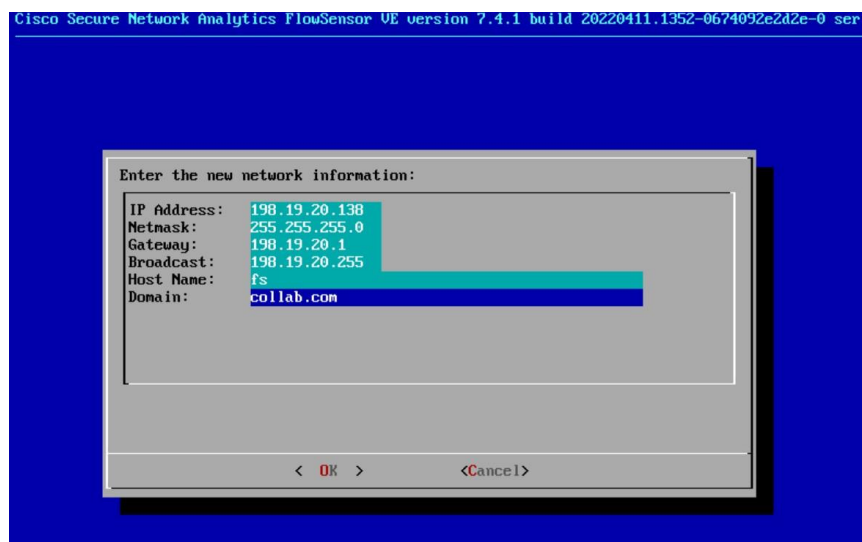


Enter the network configuration for the appliance.



Installation of Flow Sensor

Log in to the console, type the comand SystemConfig. Enter the network configuration for the appliance.



Installation of Cisco Telemetry Broker

Cisco Telemetry Broker the core component of

Cisco Secure Network Analytics (Formerly Cisco Stealthwatch) and a powerfull device to optimize telemetry, it is mainly used :

- To simplify collection and aggregation of Netflow, SNMP and Syslog traffic.
- It simplifies configuring and sending Netflow data using one exporter in your Network Devices instead of different exporters, especially when you have disparate netflow analyzers like Cisco Secure Network Analytics, SolarWinds or LiveAction, or in case you have multiple flow collectors with Cisco Secure Network Analytics.
- In addition it simplifies the Telemetry Streams when using multiple destinations and differents logs management solutions.

The architecture of Cisco Telemetry Broker consists of two components:

- Manager Node
- Broker Node.

Broker Nodes are all managed by one Cisco Telemetry Broker manager using the Management Interface. Manager Node requires one network interface for management traffic. Broker Node requires two network interfaces. One management interface for communication with the manager and the Telemetry interface to send Telemetry to Flow Collector which in turn sends to the configured destinations such as SMC Management Console in the Cisco Secure Network Analytics solution. The Destination Flow Collector

IP Address/Port of the telemetry traffic in Cisco Secure Network Analytics solution is added on the Manager Node and pushed down to the Broker Node through the management interface to instruct them where to NetFlow traffic.

When Installing the Broker Node, you must join it to the manager Node using the `sudo ctb-manage` command and provides the IP Address and admin credentials of the Manager Node. Once the Broker Node is added into the Manager Node, the Web GUI of the Manager Node displays the Broker Node added with its management IP Address. To finish the integration between the Broker Node and Manager Node, you need to add the Data or Telemetry Network Interface of the Broker Node to the Manager Node. Finally the Network Devices such as firewalls, Routers and Switches use the Broker Node Telemetry Interface IP Address as the Netflow Exporter.

Deploy the Manager Node

Run the `sudo ctb-install --init` command.

Enter the following informations :

- Password for the admin user
- Hostname
- IPv4 address, subnet mask, and default gateway address for the Management Network interface
- DNS nameserver IP address

```
admin@ctb-zhfaUuas:~$  
admin@ctb-zhfaUuas:~$ sudo ctb-install --init  
  
Starting install process for CTB Manager  
CTB Version: v1.2.2-0-g5e59a32  
  
== Setting up admin account:  
Password:█
```

Deploy the Broker Node

Run the `sudo ctb-install --init` command.

Enter the following informations :

- Password for the admin user
- Hostname
- IPv4 address, subnet mask, and default gateway address for the Management Network interface
- DNS nameserver IP address

```
admin@ctb-vnrAQ73r:~$
admin@ctb-vnrAQ73r:~$ sudo ctb-install --init
[sudo] password for admin:

Starting install process for CTB Broker Node
CTB Version: v1.2.2-0-g5e59a32

== Setting up admin account:
Password:
```

Run the sudo ctb-manage command.

Enter the following informations :

- IP address of the Manager node
- Username of the admin account of the Manager node

```
admin@ctb-vnrAQ73r:~$
admin@ctb-vnrAQ73r:~$ sudo ctb-manage

== Management Configuration

Manager node address: 198.19.20.150

== Testing connection to server exists
ctb-zhfaUuas [198.19.20.150] 443 (https) open

== Fetching certificate from 198.19.20.150
Subject Hash
6e88de4c
subject=C = US, ST = California, L = San Jose, O = Cisco Systems, OU = dCloud, CN = 198.19.20.150
issuer=C = US, ST = California, L = San Jose, O = Cisco Systems, OU = dCloud, CN = 198.19.20.150
Validity:
notBefore=Jul 27 23:01:22 2022 GMT
notAfter=Jul 24 23:01:22 2032 GMT

Do you accept the authenticity of the server? [y/n] y
== Acquiring API key from 198.19.20.150
Management UI username: admin
Management UI password:
```

Log in to Cisco Telemetry Broker. In a web browser, enter the Manager's management interface IP address of the manager node. From the main menu, choose Broker Nodes.

In the Broker Nodes table, click the broker node. In the Telemetry Interface section, Configure the Telemetry Interface et the default gateway.

Telemetry Broker Overview Destinations Sources **Broker Nodes** Manager Node Integrations

Broker Nodes Search

All (1) Unconfigured (0) Dropping Packets (0) Inactive (0) Highest Received Rate

Broker Node Name	Telemetry Interface	Capacity	Cluster	Received Rate (bps)	Sent Rate (bps)	Status
ctb-vnrAQ73r 198.19.20.151	198.19.20.139	10 G	-	611 k 0.06% of 10 G	611 k 0.06% of 10 G	✓ Sending Data Last Seen Just Now

High Availability Clusters + Add Cluster

Telemetry Broker Overview Destinations Sources **Broker Nodes** Manager Node Integrations

Broker Nodes / ctb-vnrAQ73r Remove Broker Node

ctb-vnrAQ73r

General

Hostname: ctb-vnrAQ73r

Management Network IP Address: 198.19.20.151

Status

✓ **Active**
Last Seen 30 Seconds Ago

Received Rate

611 kbps
0.06% of 10 G

Sent Rate

611 kbps
0.06% of 10 G

Telemetry Interface

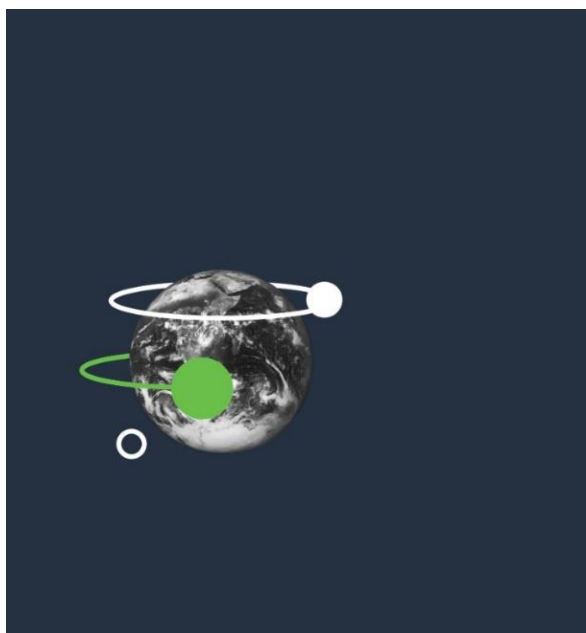
Interface Index	2	IPv4 Address/Mask	198.19.20.139/24
Interface Name	ens192	IPv4 Gateway Address	198.19.20.1
MAC Address	00:50:56:97:71:2b	IPv6 Address/Mask	-
PCI Address	0000:0b:00:0	IPv6 Gateway Address	-
Capacity (bps)	10 G		

Now the SNA appliances are configured with a management IP address, we need to complete the Appliance Setup Tool (AST) on each SNA components.

The Appliance Setup Tool (AST) will configure the appliances to be able to communicate with the rest of the SNA deployment.

SMC

- Access the SMC GUI.



Secure Network Analytics

User Name *

Password *

[Sign In](#)

- Change the Default Passwords for admin, root, and sysadmin.



Welcome to the Secure Network Analytics Appliance Setup Tool!

This tool will help you configure your Secure Network Analytics appliance step by step.

Before you begin:

- Ensure your firewalls and ACLs will allow access.
- Gather the host name for the appliance and IP addresses for the following:
 - Appliance
 - Subnet mask
 - Default and broadcast gateways
 - NTP and DNS servers
 - Manager IP Address for Central Management

For more information, refer to your Secure Network Analytics System documentation.

[Continue →](#)

Step 1: Change Default Password

Step 2: Management Network Interface

Step 3: Host Name and Domains

Step 4: DNS Settings

Step 5: NTP Settings

Step 6: Register Your Appliance

Complete

Change Default Passwords

Password Format (Case Sensitive)

- Must be between 8 and 256 characters.
- Must be different from the previous password by at least 4 characters.
- Must not be the same as the previous 12 password(s).
- Must not be similar or the same as your username.
- Must exclude dictionary words and repeated or sequential characters.
- Must consist of only ASCII symbols.

Note: You must change the password for all the users before continuing.

ADMIN

ROOT

SYSADMIN

Current Password:*

New Password:*

[Generate Password](#)

Password Strength - Medium

Confirm New Password: *

☐ Show Password

* = Required

[Back](#) [Next →](#)

Step 1:
Change Default Password

Step 2:
Management Network Interface

Step 3:
Host Name and Domains

Step 4:
DNS Settings

Step 5:
NTP Settings

Step 6:
Register Your Appliance

Complete

Change Default Passwords

Password Format (Case Sensitive)

- Must be between 8 and 256 characters.
- Must be different from the previous password by at least 4 characters.
- Must not be the same as the previous 12 password(s).
- Must not be similar or the same as your username.
- Must exclude dictionary words and repeated or sequential characters.
- Must consist of only ASCII symbols.

Note: You must change the password for all the users before continuing.

ADMINROOTSYSADMIN

Current Password:*

New Password:*

Required

Password Strength - Medium

Generate Password

Confirm New Password:

☐ Show Password

* = Required

BackNext

Step 1:
Change Default Password

Step 2:
Management Network Interface

Step 3:
Host Name and Domains

Step 4:
DNS Settings

Step 5:
NTP Settings

Step 6:
Register Your Appliance

Complete

Change Default Passwords

Password Format (Case Sensitive)

- Must be between 8 and 256 characters.
- Must be different from the previous password by at least 4 characters.
- Must not be the same as the previous 12 password(s).
- Must not be similar or the same as your username.
- Must exclude dictionary words and repeated or sequential characters.
- Must consist of only ASCII symbols.

Note: You must change the password for all the users before continuing.

ADMINROOTSYSADMIN

Current Password:*

New Password:*

Required

Password Strength - Medium

Generate Password

Confirm New Password:

☐ Show Password

* = Required

BackNext

No changes for the Management Network Interface.

Step 1:
Change Default Password

Step 2:
Management Network Interface

Step 3:
Host Name and Domains

Step 4:
DNS Settings

Step 5:
NTP Settings

Step 6:
Register Your Appliance

Complete

Management Network Interface

Enable communication between this appliance and the network. Default network settings for this appliance appear below. Before changing any of these settings, confer with your network administrator.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Interface Name: eth0

Interface MAC Address: 00:50:56:97:8c:f3

IPv4

IPv6

IP Address:* 198.19.20.136

Subnet Mask:* 255.255.255.0

Default Gateway:* 198.19.20.1

Broadcast Address:* 198.19.20.255

* = Required

Next →

Configure the Host Name and Domains.

Step 1:
Change Default Password

Step 2:
Management Network Interface

Step 3:
Host Name and Domains

Step 4:
DNS Settings

Step 5:
NTP Settings

Step 6:
Register Your Appliance

Complete

Host Name and Domains

Enter identifying information for this appliance and the network domain where it is installed.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Host Name:* smc

Network Domain:* collab.com

Identify your organization's domain and the IP addresses that Secure Network Analytics will be monitoring.

Manager Domain:* COLLAB

Manager Domain Type: * Data Store

IP Address Ranges:

10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
fc00::/7

* = Required

Next →

- Configure the DNS Servers.

Manager VE
 Appliance Setup
 Serial Number: SMCVE-VMware-42170879186938e5-0918cdf8aa198bd1
 Version: 7.4.1
 Build: 20220411.1352-0674092e2d2e-0

Step 1:
 Change Default Password

Step 2:
 Management Network Interface

Step 3:
 Host Name and Domains

Step 4:
 DNS Settings

Step 5:
 NTP Settings

Step 6:
 Register Your Appliance

Complete

DNS Settings

Enter the IP address(es) of your domain name server(s). To add a server, click the + button. To delete a server, select the corresponding checkbox, and then click the - button.

Delete	DNS Server
<input type="checkbox"/>	198.19.20.10
<input type="checkbox"/>	198.19.20.134

* = Required

- Configure the NTP Server.

Manager VE
 Appliance Setup
 Serial Number: SMCVE-VMware-42170879186938e5-0918cdf8aa198bd1
 Version: 7.4.1
 Build: 20220411.1352-0674092e2d2e-0

Step 1:
 Change Default Password

Step 2:
 Management Network Interface

Step 3:
 Host Name and Domains

Step 4:
 DNS Settings

Step 5:
 NTP Settings

Step 6:
 Register Your Appliance

Complete

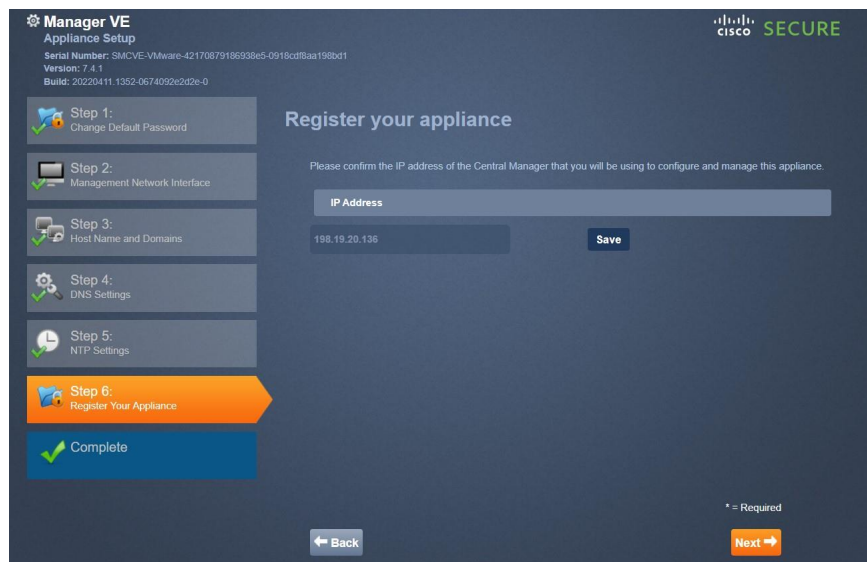
NTP Settings

Select or enter the IP address(es) or name(s) of your network time protocol server(s). Choose the same NTP server(s) used for other devices that feed information to the Flow Collector for NetFlow. To add a server, click the + button. To delete a server, select the corresponding checkbox, and then click the - button.

Delete	NTP Server
<input type="checkbox"/>	198.18.128.1

* = Required

- Finally register the SMC.



- The SMC will reboot.

Datastore Node

Follow the same procedure, the only difference is the configuration of Central Management Settings. In this section Enter the IP address of SMC 198.19.20.136 and the username/password.

Flow Collector

Follow the same procedure, the only difference is the configuration of Central Management Settings. In this section Enter the IP address of SMC 198.19.20.136 and the username/password.

Flow Sensor

- Follow the same procedure, the only difference is the configuration of Central Management Settings. In this section Enter the IP address of SMC 198.19.20.136 and the username/password.
- To complete the configuration, Initialize the DataStore node.
- SSH to the DataStore node and run the SystemConfig command.
- Follow the interactive dialog to initialize the DataStore node.
- Access the SMC GUI, in the Central Management we can see all Cisco SNA appliances are connected to SMC.

Central Management

Appliance Manager

Data Store

Update Manager

App Manager

Smart Licensing

Inventory

4 Appliances found

Appliance Status	Host Name	Type	IP Address	Actions
Connected	datastore	Data Node DNODEVE-VMware-4217b62bb73738ef-3ac22bd579b65ccd	198.19.20.101	...
Connected	fcnf	Flow Collector Data Store FCNFVE-VMware-4217b62bb73738ef-3ac22bd579b65bbc	198.19.20.137	...
Connected	fs	Flow Sensor FSVE-VMware-42173a464eb01a9f-f0452db1e75acf25	198.19.20.138	...
Connected	smc	Manager SMCVE-VMware-42170879186938e5-0918cdf8aa198bd1	198.19.20.136	...

Cisco Telemetry Broker Configuration

Access the Cisco Telemetry Broker Manager node GUI. Click Add Destination and select UDP Destination. Configure the following parameters.

- Destination Name: SNA-FC
- Destination IP Address: 198.19.20.137
- Destination UDP Port: 2055

Telemetry Broker

OverviewDestinationsSourcesBroker NodesManager NodeIntegrations

Destinations

No destinations have been configured

You can export your current UDP Director destination and rules configuration as an XML file and import it into Telemetry Broker.

Upload XML File

Alternatively, you can manually add a destination to Telemetry Broker.

Add Destination

- UDP Destination
- SCA Destination

Telemetry Broker

OverviewDestinationsSourcesBroker NodesManager NodeIntegrations

Destinations

Add Destination

Destination Name

SNA-FC

Destination IP Address

198.19.20.137

Destination UDP Port

2055

Use either IPv4 or IPv6 format.

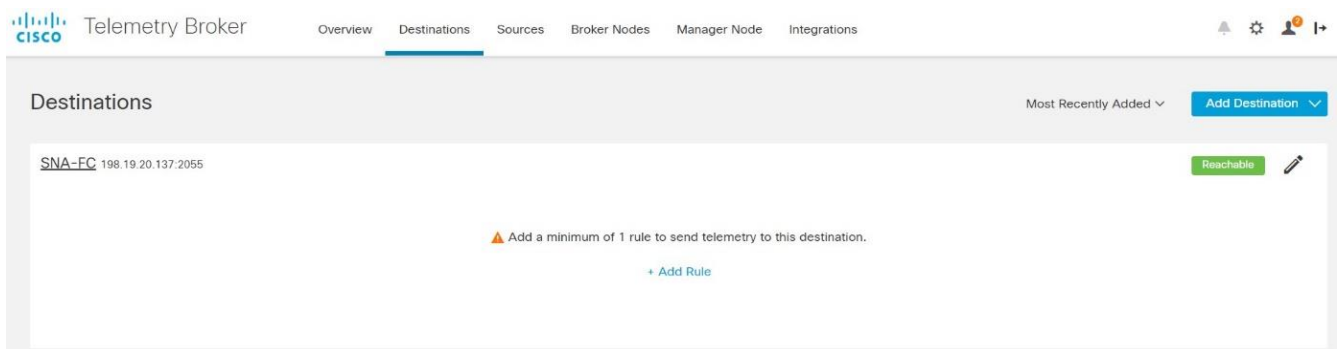
Check Destination Reachability

Allows Telemetry Broker to detect non-responsive destinations. Disable this if your destination or firewall rule configuration will result in false positive alerts.

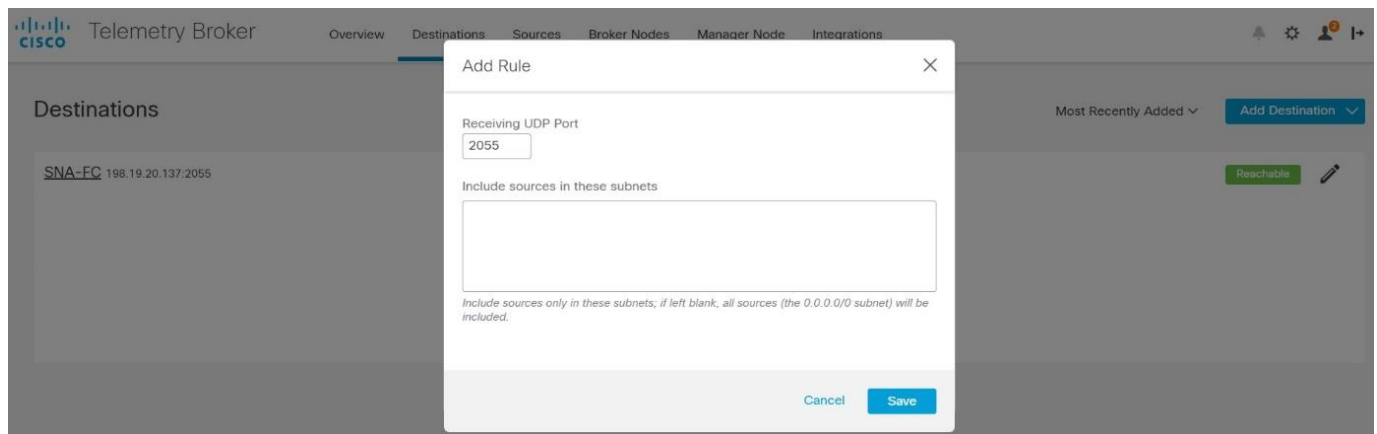
Cancel

Save

Click Add Rule.



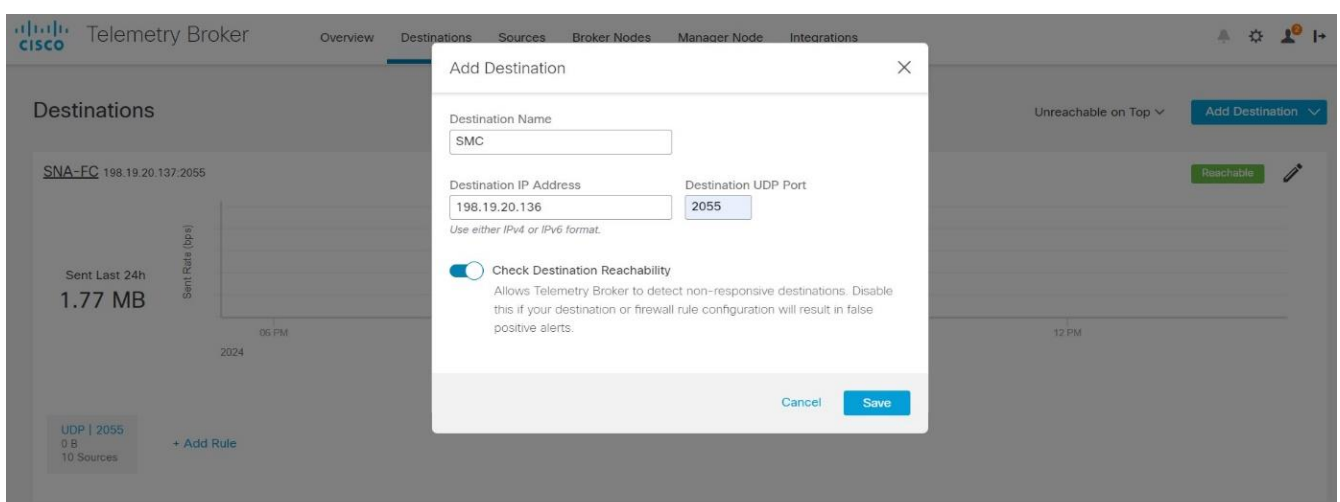
- Enter 2055 as the Receiving UDP Port.



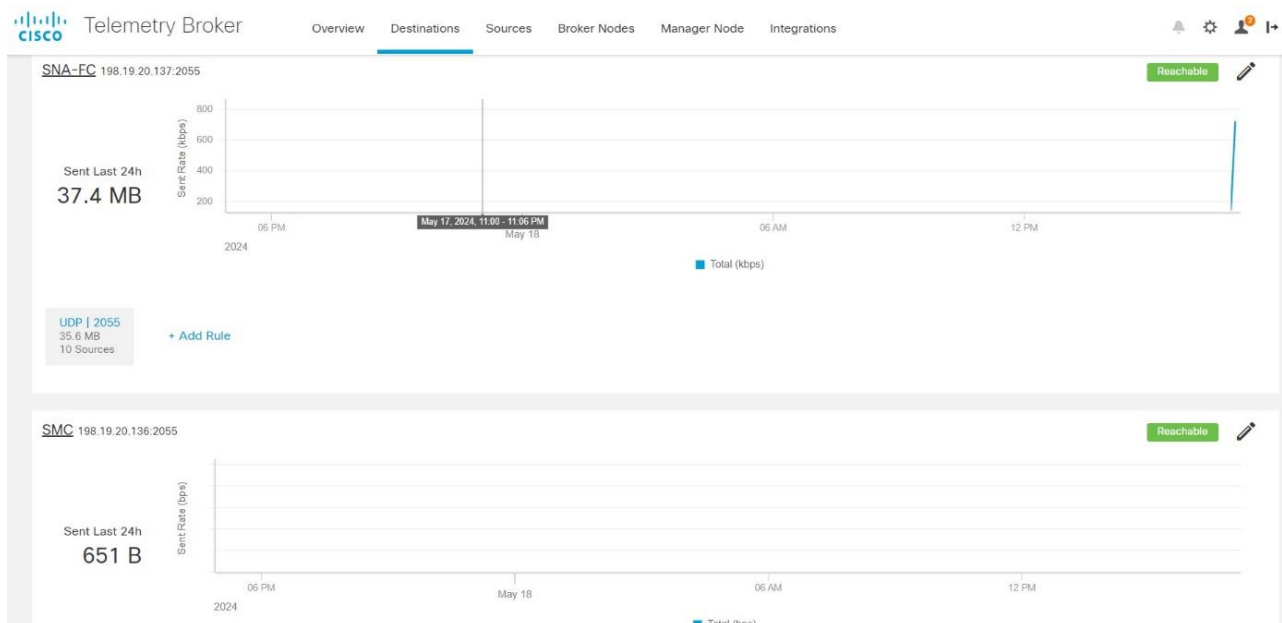
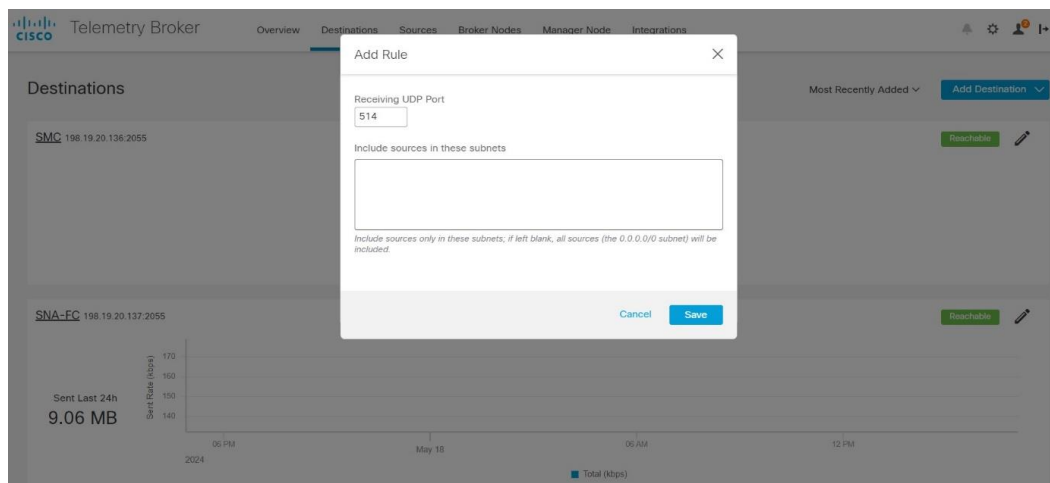
Click Add Destination and select UDP Destination.

Configure the following parameters.

- Destination Name: Manager
- Destination IP Address: 198.19.20.136
- Destination UDP Port: 514



- Click Add Rule.
- Enter 2055 as the Receiving UDP Port.



Cisco ISE Identity Services Engine Integration

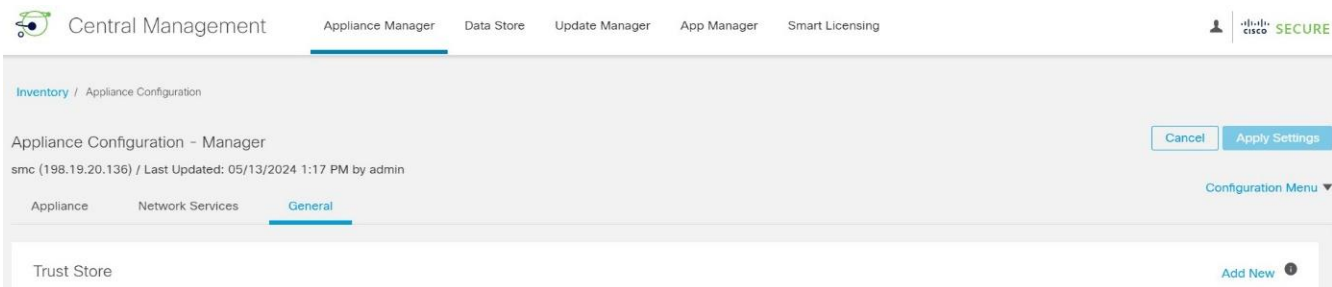
Navigate to Administration > pxGrid > Certificates.

Complete the form as follows:

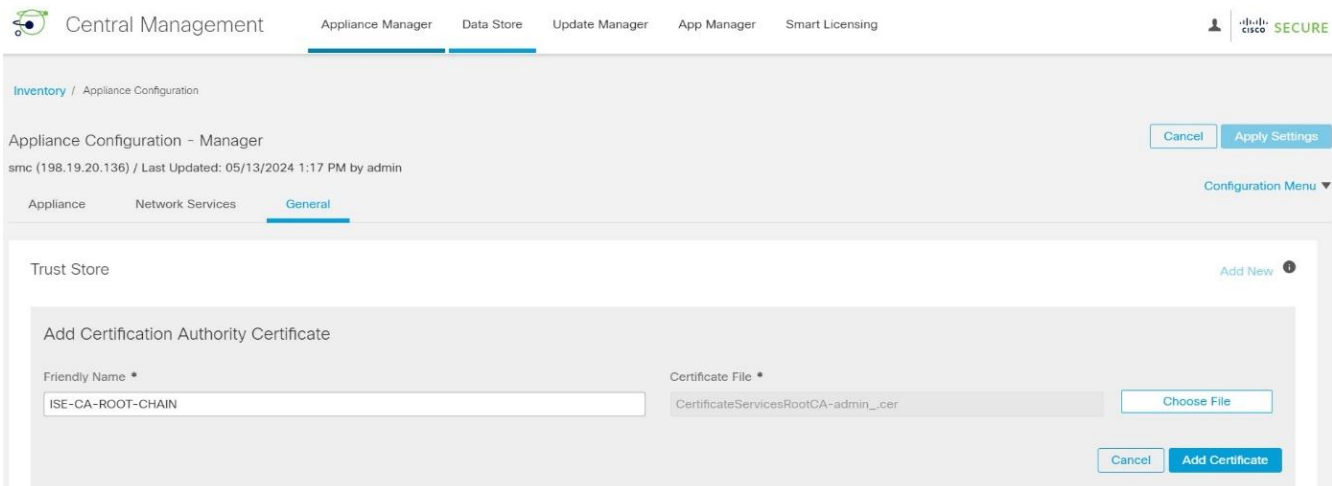
- Click in the I want to field and select Download Root Certificate Chain
- Click in the Host Names field and select admin
- Click in the Certificate Download Format field and select the PEM option
- Click Create

- Download the file as ISE-CA-ROOT-CHAIN.zip.

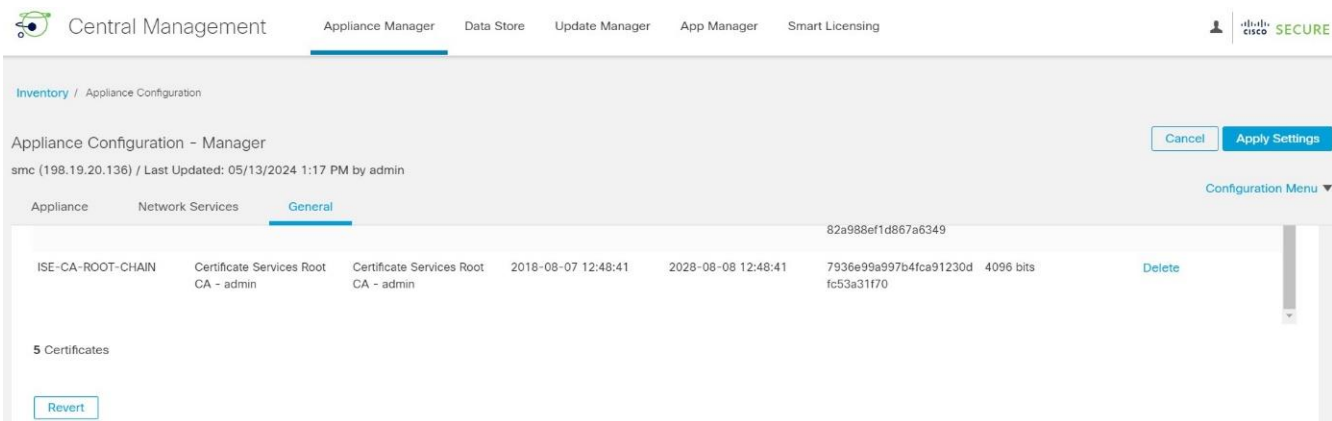
- On the SMC GUI, click Central Management. On the Central Management page, locate the SMC Manager appliance, then select Edit Appliance Configuration.
- Click General.



- Scroll down to Trust Store and click Add New. Select the CertificateServicesRootCA-admin_.cer file. Click Add Certificate.



- The SMC will now trust certificates issued by the ISE CA.



- Click the Appliance tab. Scroll down to Additional SSL/TLS Client Identities section and click Add New.

Central Management Appliance Manager Data Store Update Manager App Manager Smart Licensing SECURE

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

smc (198.19.20.136) / Last Updated: 05/13/2024 1:17 PM by admin

Appliance Network Services General Configuration Menu

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length
smc	smc.dcloud.cisco.com	smc.dcloud.cisco.com	2024-05-12 11:24:37	2029-05-13 11:24:37	2fd8df9ec183f45fb06d8a71e5f0607e1d24aee	8192 bits

Additional SSL/TLS Client Identities Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
There is no data to display							

- It will ask if you need to generate a CSR, select Yes and click Next.

Central Management Appliance Manager Data Store Update Manager App Manager Smart Licensing SECURE

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

smc (198.19.20.136) / Last Updated: 05/13/2024 1:17 PM by admin

Appliance Network Services General Configuration Menu

Do you need to generate a CSR?

☒ Yes

☐ No

Cancel Next

⚠ Your certificates are critical for your system's security. Improperly modifying your certificates can break your system. Follow the instructions in the [Help](#) to update the Additional SSL/TLS Client Identities.

Fill out the CSR as follows:

- RSA Key Length
- Organization
- Organizational Unit
- Locality or City
- State or Province
- Country Code
- Email Address

Click Generate CSR, then Download CSR.

Central Management | Appliance Manager | Data Store | Update Manager | App Manager | Smart Licensing |

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

smc (198.19.20.136) / Last Updated: 05/13/2024 1:17 PM by admin

Appliance | Network Services | General Configuration Menu ▼

Generate a CSR

RSA Key Length *

☐ 2048 bits

☒ 4096 bits

☐ 8192 bits

Common Name

smc.dcloud.cisco.com

Organization

Security IT

Organizational Unit

Security Analyst

Locality Or City

San Jose

State Or Province

California

Country Code

US

Email Address

Central Management | Appliance Manager | Data Store | Update Manager | App Manager | Smart Licensing |

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

smc (198.19.20.136) / Last Updated: 05/13/2024 1:17 PM by admin

Appliance | Network Services | General Configuration Menu ▼

Additional SSL/TLS Client Identities ⓘ

Add SSL/TLS Client Identity Download CSR

Friendly Name *

Certificate File *

Choose File

Cancel Add Client Identity

Access the Cisco ISE GUI. Navigate to Administration > pxGrid > Certificates.

Use the following informations :

- In the I want to field, select Generate a single certificate (with certificate signing request)
- Past the CSR in the Certificate Signing Request Details field
- Type SMC in the Description field
- Select IP Address in the SAN field and enter 198.19.20.136 as the associated IP Address
- Select PKCS12 format as the Certificate Download Format option
- Enter a password
- Click Create

- Save the certificate created with a name SMC-PXGRID.

Note :

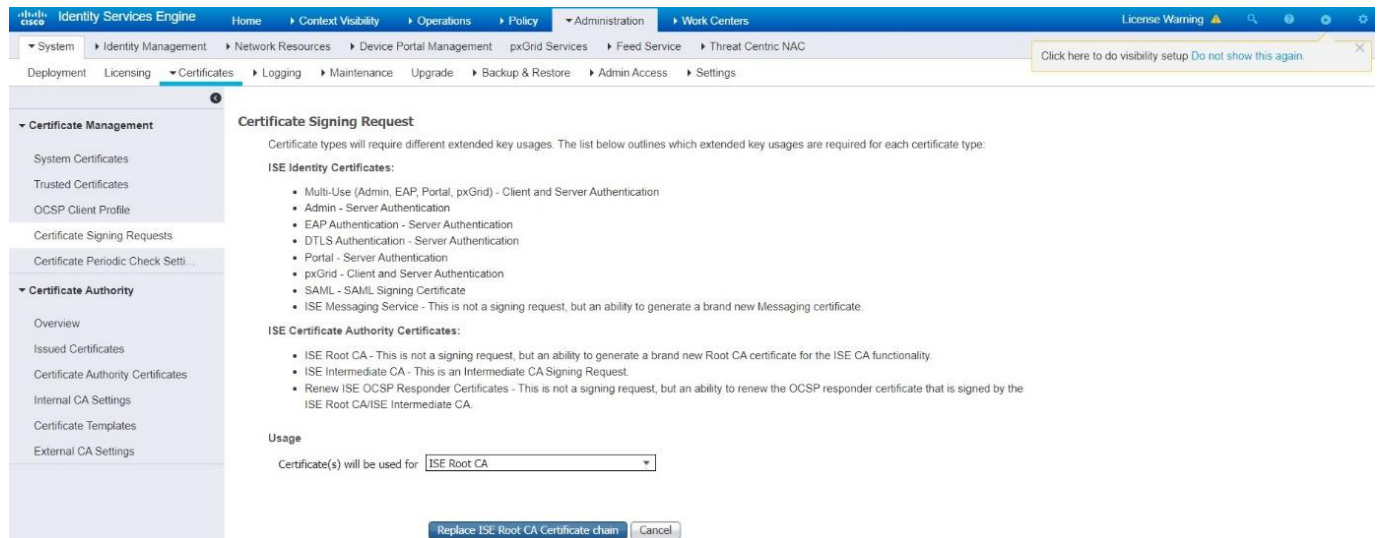
In some existing Cisco ISE deployment, you may have expired system certificates used for admin, eap and pxGrid services as shown below.

	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
<input type="checkbox"/>	Certificate Services Root CA - admin#00001	Enabled	Infrastructure, Cisco Services, Endpoints, AdminAuth	79 36 E9 9A 99 7B 4F CA 91 23 0D FC 53 A3 1F 70	Certificate Services Root CA - admin	Certificate Services Root CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2028	✓
<input type="checkbox"/>	Certificate Services Node CA - admin#00002	Enabled	Infrastructure, Endpoints, AdminAuth	79 EA 0E 6E 52 85 43 C8 82 BE 2D C8 74 D4 CE 33	Certificate Services Node CA - admin	Certificate Services Root CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
<input type="checkbox"/>	Certificate Services Endpoint Sub CA - admin#00003	Enabled	Endpoints, AdminAuth, Infrastructure	63 B0 83 05 FD 58 42 84 B7 67 A5 FA FA FE F9 32	Certificate Services Endpoint Sub CA - admin	Certificate Services Node CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
<input type="checkbox"/>	Certificate Services OSCP Responder - admin#00004	Enabled	Infrastructure, Endpoints, AdminAuth	70 BB DF D7 A4 B3 4F AD B5 17 5C E0 33 49 42 01	Certificate Services OSCP Responder - admin	Certificate Services Node CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗

This is because the Cisco ISE internal CA certificates that sign these system certificates are expired.

	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
<input type="checkbox"/>	Certificate Services Root CA - admin#00001	Enabled	Unknown	79 36 E9 9A 99 7B 4F CA 91 23 0D FC 53 A3 1F 70	Certificate Services Root CA - admin	Certificate Services Root CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2028	✓
<input type="checkbox"/>	Certificate Services Node CA - admin#00002	Enabled	Unknown	79 EA 0E 6E 52 85 43 C8 82 BE 2D C8 74 D4 CE 33	Certificate Services Node CA - admin	Certificate Services Root CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
<input type="checkbox"/>	Certificate Services Endpoint Sub CA - admin#00003	Enabled	Unknown	63 B0 83 05 FD 58 42 84 B7 67 A5 FA FA FE F9 32	Certificate Services Endpoint Sub CA - admin	Certificate Services Node CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
<input type="checkbox"/>	Certificate Services OSCP Responder - admin#00004	Enabled	Unknown	70 BB DF D7 A4 B3 4F AD B5 17 5C E0 33 49 42 01	Certificate Services OSCP Responder - admin	Certificate Services Node CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
<input type="checkbox"/>	Certificate Services Root CA - admin#00005	Enabled	Infrastructure, Cisco Services, Endpoints, AdminAuth	21 48 0F D2 AC 19 4F D6 A9 8D 84 69 06 6C DB 3C	Certificate Services Root CA - admin	Certificate Services Root CA - admin	Wed, 15 May 2024	Tue, 16 May 2034	✓
<input type="checkbox"/>	Certificate Services Node CA - admin#00006	Enabled	Infrastructure, Endpoints, AdminAuth	2D 81 90 BE E8 E7 48 AB 96 23 36 1C B2 B4 87 0E	Certificate Services Node CA - admin	Certificate Services Root CA - admin	Wed, 15 May 2024	Tue, 16 May 2034	✓
<input type="checkbox"/>	Certificate Services Endpoint Sub CA - admin#00007	Enabled	Infrastructure, Endpoints, AdminAuth	7D 66 2A 64 37 75 4B 75 96 A8 1E 90 3D 64 DB 48	Certificate Services Endpoint Sub CA - admin	Certificate Services Node CA - admin	Wed, 15 May 2024	Tue, 16 May 2034	✓
<input type="checkbox"/>	Certificate Services OSCP Responder - admin#00008	Enabled	Infrastructure, Endpoints, AdminAuth	02 C8 89 6F EB 8D 4A AD BE 26 15 B4 17 48 32 24	Certificate Services OSCP Responder - admin	Certificate Services Node CA - admin	Wed, 15 May 2024	Wed, 16 May 2029	✓

To renew the system certificates. Navigate to Administration > Certificates > Certificate Signing Requests. In the Usage field, select ISE Root CA, then click on Replace ISE Root CA Certificate Chain.



Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - This is not a signing request, but an ability to generate a brand new Messaging certificate.

ISE Certificate Authority Certificates:

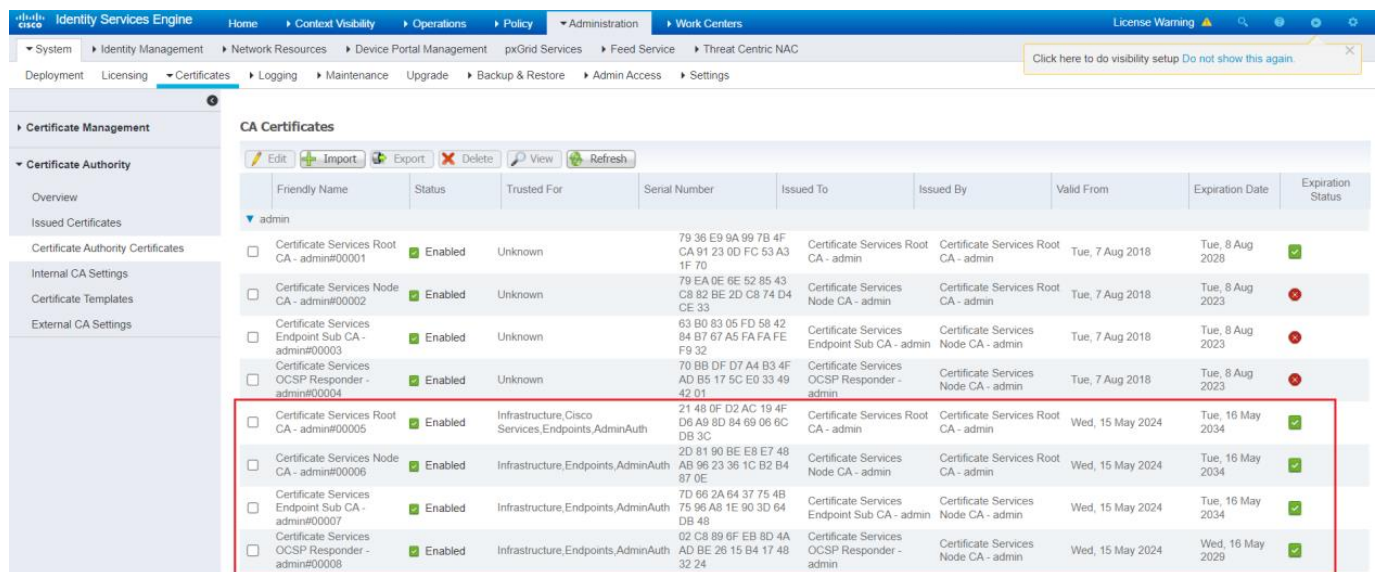
- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: ISE Root CA

[Replace ISE Root CA Certificate chain](#) [Cancel](#)

The Cisco ISE generate a new Internal CA certificates. Dont forget to adjust the Trusted For field for the appropriate services such as pxGrid.



CA Certificates

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Certificate Services Root CA - admin#00001	Enabled	Unknown	79 36 E9 9A 99 7B 4F CA 91 23 0D FC 53 A3 1F 70	Certificate Services Root CA - admin	Certificate Services Root CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2028	✓
Certificate Services Node CA - admin#00002	Enabled	Unknown	79 EA DE 6E 52 85 43 C8 82 BE 2D C8 74 D4 CE 33	Certificate Services Node CA - admin	Certificate Services Root CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
Certificate Services Endpoint Sub CA - admin#00003	Enabled	Unknown	63 B0 83 05 FD 58 42 84 B7 67 A5 FA FE F9 32	Certificate Services Endpoint Sub CA - admin	Certificate Services Node CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
Certificate Services OCSP Responder - admin#00004	Enabled	Unknown	70 BB DF D7 A4 B3 4F AD B5 17 5C E0 33 49 42 01	Certificate Services OCSP Responder - admin	Certificate Services Node CA - admin	Tue, 7 Aug 2018	Tue, 8 Aug 2023	✗
Certificate Services Root CA - admin#00005	Enabled	Infrastructure, Cisco Services, Endpoints, AdminAuth	21 48 0F D2 AC 19 4F D6 A9 8D 84 69 06 6C DB 3C	Certificate Services Root CA - admin	Certificate Services Root CA - admin	Wed, 15 May 2024	Tue, 16 May 2034	✓
Certificate Services Node CA - admin#00006	Enabled	Infrastructure, Endpoints, AdminAuth	2D 81 90 BE E9 E7 48 AB 96 23 36 1C B2 B4 87 0E	Certificate Services Node CA - admin	Certificate Services Root CA - admin	Wed, 15 May 2024	Tue, 16 May 2034	✓
Certificate Services Endpoint Sub CA - admin#00007	Enabled	Infrastructure, Endpoints, AdminAuth	7D 66 2A 64 37 75 4B 75 96 A8 1E 90 3D 64 DB 48	Certificate Services Endpoint Sub CA - admin	Certificate Services Node CA - admin	Wed, 15 May 2024	Tue, 16 May 2034	✓
Certificate Services OCSP Responder - admin#00008	Enabled	Infrastructure, Endpoints, AdminAuth	02 C8 89 6F EB 8D 4A AD BE 26 15 B4 17 48 32 24	Certificate Services OCSP Responder - admin	Certificate Services Node CA - admin	Wed, 15 May 2024	Wed, 16 May 2029	✓

Now the system certificates are valid.

- Client Name: SMC-PXGRID

Network Analytics

FETRAINI...

Data Store

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

SEARCH

USER

SETTINGS

CISCO SECURE

Cisco ISE Configuration Setup

Cancel

Save

Connection Details

Integration options

Cluster Name: *
ISE-CLUSTER

Certificate: *
SMC-PXGRID

PxGrid Node 1: *
198.19.20.141

PxGrid Node 2:
ex. 10.10.10.10 or pxgrid.ise.cisco.com

PxGrid Node 3:
ex. 10.10.10.10 or pxgrid.ise.cisco.com

Client Name: *
SMC-PXGRID

☒ Enable strict ISE Server Identity Verification

Integrated Product

☒ Cisco ISE

☐ Cisco ISE PIC (Passive Identity Connector)

☒ Adaptive Network Control

☒ Static SGT Classifications

☒ Sessions

☐ Track sessions derived from machine authentications

Network Analytics

FETRAINI...

Data Store

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

SEARCH

USER

SETTINGS

CISCO SECURE

Cisco® ISE Configuration

Cisco® ISE Configuration

Add new configuration

Cluster Name	PxGrid Nodes	User Name	Status	Actions
ISE-CLUSTER	198.19.20.141 ...	SMC-PXGRID	● ↺	...

Network Analytics

FETRAINI...

Data Store

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

SEARCH

USER

SETTINGS

CISCO SECURE

Cisco® ISE Configuration

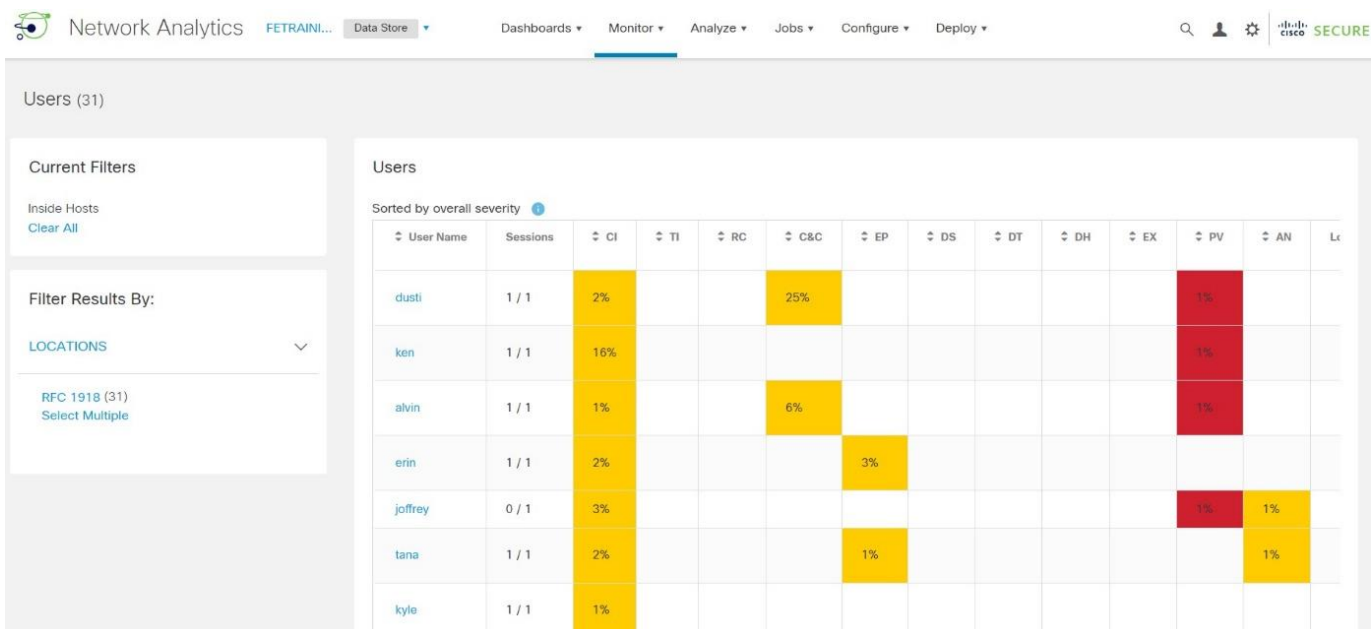
Cisco® ISE Configuration

Add new configuration

Cluster Name	PxGrid Nodes	User Name	Status	Actions
ISE-CLUSTER	198.19.20.141 ...	SMC-PXGRID	● ↺	...

Navigate to Monitor > Users.

Notice that we can see User data on SMC.



ISE Adaptive Network Control (ANC) Policies

Select Operations > Adaptive Network Control > Policy List > Add and enter SW_QUARANTINE for the Policy Name and Quarantine for the Action.

Identity Services Engine Home ▾ Context Visibility ▾ Operations ▾ Policy ▾ Administration ▾ Work Centers ▾ License Warning ⚠

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot ▾ Adaptive Network Control Reports

Policy List Endpoint Assignment

List > New

Input fields marked with an asterisk (*) are required.

Name * SW_Quarantine

Action * QUARANTINE

Cancel Submit

Identity Services Engine Home ▾ Context Visibility ▾ Operations ▾ Policy ▾ Administration ▾ Work Centers ▾ License Warning ⚠

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot ▾ Adaptive Network Control Reports

Policy List Endpoint Assignment

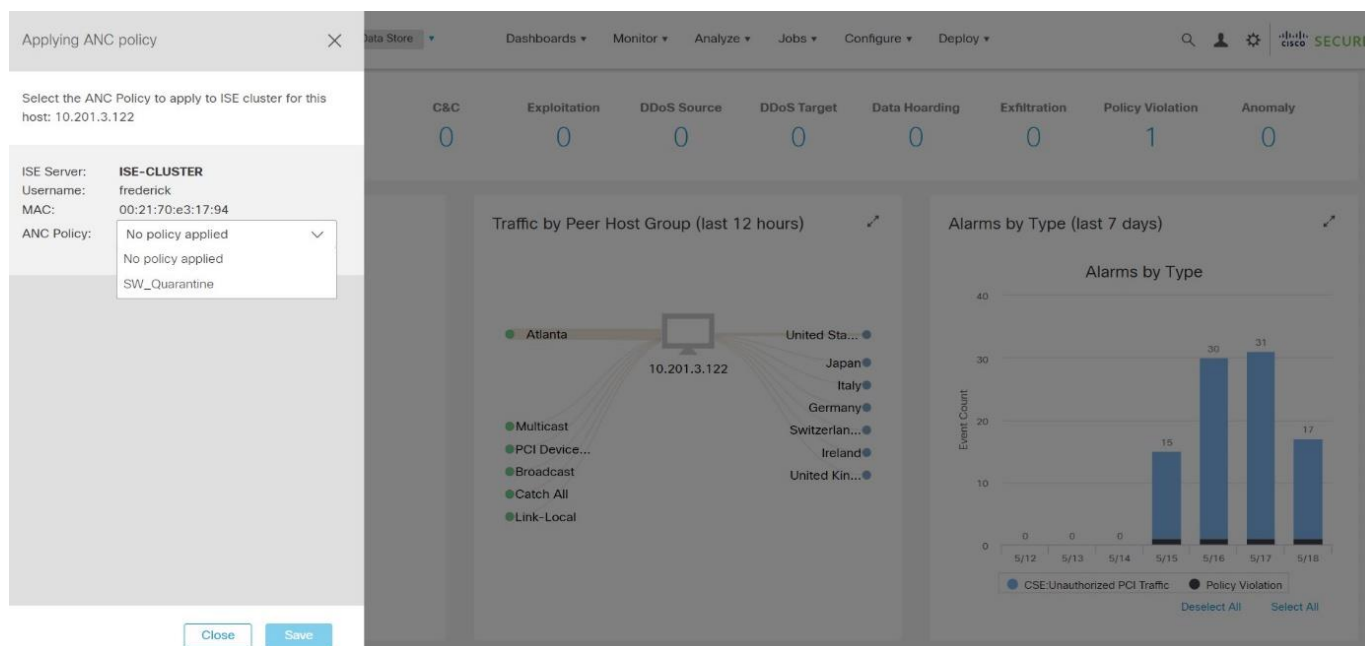
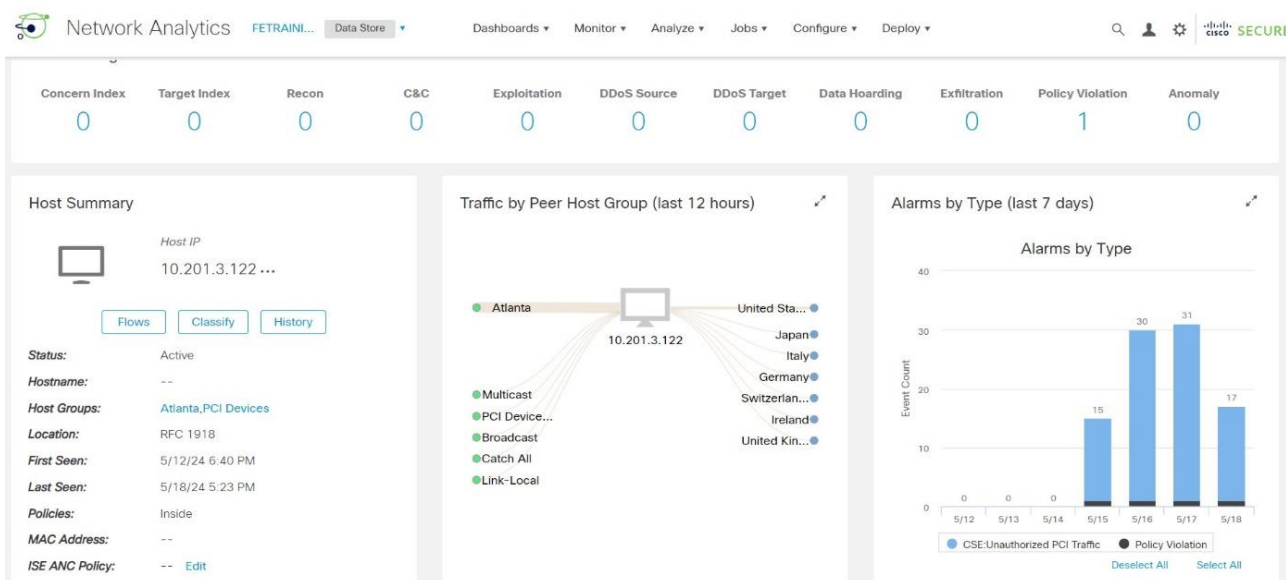
List

0 Selected

Refresh Add Trash Edit

Policy Name	ANC Actions
SW_Quarantine	QUARANTINE

Access the SMC GUI. Select an IP address in the dashboard, we can see that the ISE ANC Policy is populated.



ISE Authorization Policies

- Global authorization exception policies enable you to define rules that override all authorization rules in all of your policy sets. Once you configure a global authorization exception policy, it is added to all policy sets.
- The local authorization exception rule overwrites the global exception rules. So the local exception rule is processed first, then the global exception rule, and finally, the normal rule of the authorization policy.
- One of the interesting use case of these Exception Rules is when you configure Cisco Secure Network Analytics (Stealth watch) with Cisco ISE for Response Management using Adaptive Network Policy (ANC) so that when an alarm is raised, Cisco Secure Network Analytics (Stealth watch) will request Cisco ISE to quarantine the host with Adaptive Network Control Policy through Px Grid.

- The best practice to configure the Authorization Policy on Cisco ISE to quarantine the host either in the Local Exception or Global Exception.
- If you want to apply the ANC Policy to all your policy sets, VPN, wired wireless aka all wired VPN and wireless users. Use the Global Exception.
- If you want to apply the ANC Policy only to VPN users or Wired users. Use the Local Policy inside the VPN Policy Sets or Wired Policy Set respectively.

The screenshot shows the Cisco Identity Services Engine (ISE) Policy configuration interface. The 'Policy' tab is selected, and the 'Policy Elements' section is expanded. Under 'Authorization Policy - Local Exceptions (0)', a rule named 'ANC Quarantine Local' is highlighted with a red box. It has a status of 'On', a condition 'Session ANCPolicy EQUALS SW_Quarantine', and a result of 'DenyAccess'. Below it, under 'Authorization Policy - Global Exceptions (0)', a rule named 'ANC Quarantine Global' is highlighted with a blue box. It also has a status of 'On', the same condition, and the same result. The interface includes a search bar and a table with columns for Status, Rule Name, Conditions, Results, Profiles, and Security Groups.

Automatic Action and Response with ANC

Scenario : A company is using Cisco Umbrella as the DNS server to prevent internet threats. We want a custom alarm so that when internal users are using other external DNS servers, an alarm is triggered to prevent connection to rogue DNS servers that potentially redirect traffic to external sites for malicious purposes. When an alarm is raised, Cisco Secure Network Analytics will request Cisco ISE to quarantine the host that uses rogue DNS Servers with Adaptive Network Control Policy through PxGrid. Navigate to Configure > Host Management. In the parent host group Inside Hosts, create a Host Group named Corporate Networks for your internal networks.

Network Analytics

dcloud

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

Host Group Management

Filter by Host Group Name

dcloud

Inside Hosts

Outside Hosts

Authorized to Protected Assets

Bogon

Command & Control Servers

Tor

Import All

Export All

New Host Group

Host Group Name *

Corporate Networks

Parent Host Group

Inside Hosts

Description (512 Char Max)

IP Addresses And Ranges

198.19.30.0/24

Import IP Addresses and Ranges

In the parent host group Outside Hosts, create a Host Group named Umbrella DNS Servers for Umbrella IP addresses.

Network Analytics

dcloud

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

Host Group Management

Filter by Host Group Name

dcloud

Inside Hosts

Catch All

AHGA Inside

Business Units

By Function

By Location

Compliance Systems

Confidential Servers

Corporate Networks

Industry Reporting

Protected Asset Monitoring

Trapped Hosts - Honeypot

Outside Hosts

Authorized to Protected Assets

Bogon

Command & Control Servers

Tor

Import All

Export All

New Host Group

Host Group Name *

Umbrella DNS Servers

Parent Host Group

Outside Hosts

Description (512 Char Max)

IP Addresses And Ranges

208.67.222.222
208.67.220.220
208.67.220.222
208.67.222.220
2620:119:35::35
2620:119:53::53

Import IP Addresses and Ranges

The internal users are using Cisco Umbrella as the DNS server to prevent internet threats. Configure a custom alarm so that when internal users are using other external

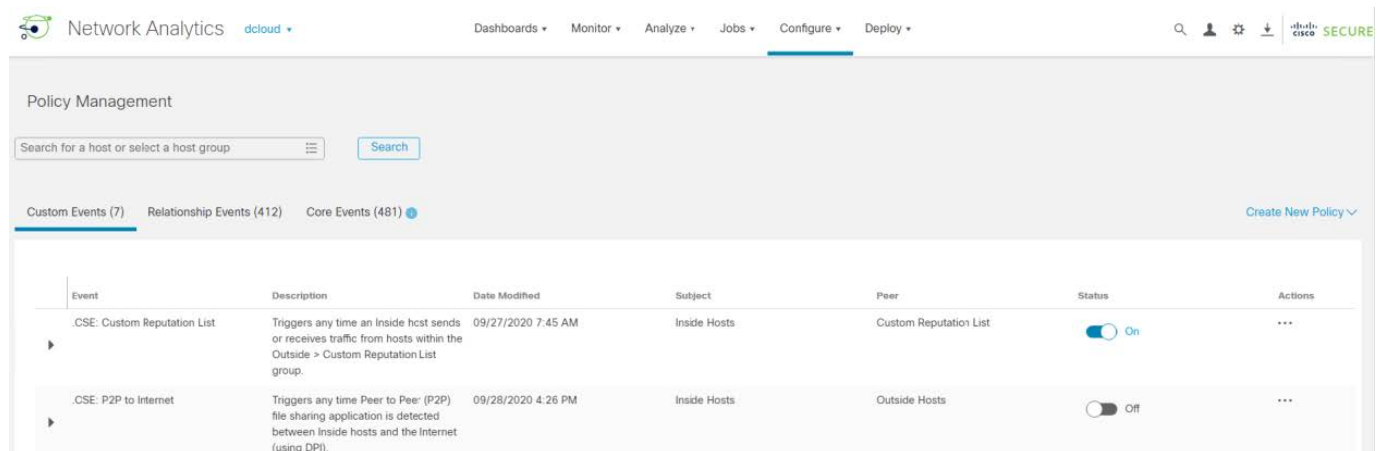
DNS servers, an alarm is triggered to prevent connection to rogue DNS server that potentially redirect traffic to external sites for malicious purposes. When an alarm is raised, Cisco Secure Network Analytics will request Cisco ISE to quarantine the host that uses rogue DNS Servers with Adaptive Network Control Policy through PxGrid.

Navigate to Configure > Policy Management.

Create a Custom Events with the following informations :

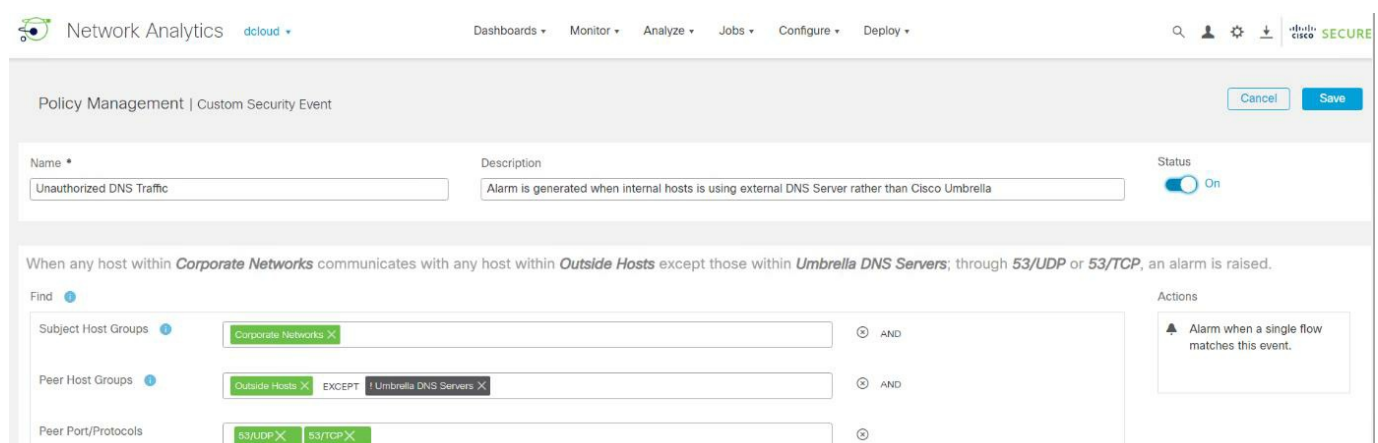
- Name : Unauthorized DNS Traffic
- Subject Host Groups : Corporate Networks
- Peer Host Groups : Outside Host Except Umbrella DNS Servers
- Peer Port/Protocols : 53/UDP 53/TCP

Basically this event is triggered when any host withing Corporate Networks Host Group communicates with any host within Outside Hosts Host Group except those within Umbrella DNS Servers Host Group, through 53/UDP or 53/TCP, an alarm is raised.



The screenshot shows the 'Policy Management' section of the Cisco Secure Network Analytics interface. It includes a search bar and tabs for 'Custom Events (7)', 'Relationship Events (412)', and 'Core Events (481)'. A table lists two custom events:

Event	Description	Date Modified	Subject	Peer	Status	Actions
.CSE: Custom Reputation List	Triggers any time an Inside host sends or receives traffic from hosts within the Outside > Custom Reputation List group.	09/27/2020 7:45 AM	Inside Hosts	Custom Reputation List	On	...
.CSE: P2P to Internet	Triggers any time Peer to Peer (P2P) file sharing application is detected between Inside hosts and the Internet (using DPI).	09/28/2020 4:26 PM	Inside Hosts	Outside Hosts	Off	...



The screenshot shows the 'Custom Security Event' configuration page. It includes fields for Name, Description, and Status. Below these, a logic builder defines the event conditions:

When any host within **Corporate Networks** communicates with any host within **Outside Hosts** except those within **Umbrella DNS Servers**; through **53/UDP** or **53/TCP**, an alarm is raised.

The configuration is as follows:

- Subject Host Groups: Corporate Networks
- Peer Host Groups: Outside Hosts EXCEPT Umbrella DNS Servers
- Peer Port/Protocols: 53/UDP, 53/TCP

The Status is set to On. An action is defined: Alarm when a single flow matches this event.

Navigate to Configure > Response Management. Click on Actions.

Network Analytics dcloud ▾

Dashboards ▾ Monitor ▾ Analyze ▾ Jobs ▾ **Configure ▾** Deploy ▾

Response Management

Rules **Actions** Syslog Formats

Actions Add New Action ▾

Name ↑	Type	Description	Used By Rules	Enabled	Actions
Auto Mitigation - Source Host	ISE ANC Policy	Automatically quarantine the offending source host leveraging an ISE ANC policy action.	1	<input checked="" type="checkbox"/>	...
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>	...
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>	...

Select the ISE ANC Policy Action. Give a name and select the Cisco ISE cluster that should be contacted to apply a quarantine policy for any violation or connection to rogue servers.

Network Analytics dcloud ▾

Dashboards ▾ Monitor ▾ Analyze ▾ Jobs ▾ **Configure ▾** Deploy ▾

Response Management

Rules **Actions** Syslog Formats

ISE ANC Policy Action Cancel Save

Name Description

☒ Enabled Disabled actions are not performed for any associated rules.

ISE Cluster

ANC Policy

Apply To ☒ Source Host ☐ Target Host

Response Management

Rules **Actions** Syslog Formats

Actions Add New Action ▾

Name ↑	Type	Description	Used By Rules	Enabled	Actions
Auto Mitigation - Source Host	ISE ANC Policy	Automatically quarantine the offending source host leveraging an ISE ANC policy action.	1	<input checked="" type="checkbox"/>	...
ISE ANC For Corporate Users	ISE ANC Policy		0	<input checked="" type="checkbox"/>	...
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>	...
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>	...

Under the Rules section. Create a new Rule. This rule will apply the previously Action when any host inside the internal network is trying to send DNS traffic to rogue DNS Servers. In the section Rule is triggered if, select Type, scroll down and select the

custom event created previously. Under the Associated Actions, select the ISE ANC action created previously.

Name: Auto Quarantine with Cisco ISE ANC

Description:

☒ Enabled Disabled rules are not triggered even when associated conditions are met.

Rule is triggered if:

ANY of the following is true:

- Type is Unauthorized DNS Traffic

Associated Actions

Execute the following actions when the alarm becomes active:

Name ↑	Type	Description	Used By Rules	Assigned
Auto Mitigation - Source Host	ISE ANC Policy	Automatically quarantine the offending source host leveraging an ISE ANC policy action.	1	<input type="checkbox"/>
ISE ANC For Corporate Users	ISE ANC Policy		0	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>

From an inside host, open the CMD console. Execute the nslookup command, then server 8.8.8.8 command. Type in a few addresses for the 8.8.8.8 DNS server to resolve.

```
cmd.exe - nslookup

> server 8.8.8.8
Default Server: dns.google
Address: 8.8.8.8

> www.cisco.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2a02:26f0:fd00:591::b33
           2a02:26f0:fd00:59f::b33
           2.22.15.111
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net

> www.amazon.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: e15316.dsca.akamaiedge.net
Addresses: 2a02:26f0:fd00:595::3bd4
           2a02:26f0:fd00:582::3bd4
           13.224.247.127
Aliases: www.amazon.com
          tp.47cf2c8c9-frontier.amazon.com
          www.amazon.com.edgekey.net

> www.twitter.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: twitter.com
Addresses: 104.244.42.65
           104.244.42.1
Aliases: www.twitter.com

>
>
```

Navigate to Monitor > ISE ANC Policy Assignments. You should see that the Cisco Secure Network Analytics applied Adaptive Network Control Policy through PxGrid and ISE to quarantine the Host.

ISE ANC Policy Assignments


<input type="checkbox"/>	Host IP Address	ISE Cluster	MAC Address	Assignment Mode	Requested By	Time	Requested ANC Policy	Effective ANC Policy	Assign ANC Policy
<input type="checkbox"/>	198.19.30.36	dCloud ISE		Automatic	(Response Management)	2/23/2023 8:55 AM	SW_Quarantine	Retrieve	...

FAQ

Q: How do I complete the Appliance Setup Tool (AST) on each SNA component?

A: Once SNA appliances are configured with a management IP address, you can complete the AST on each component by following the specific instructions provided for that component within the user manual or setup guide.

Documents / Resources



[CISCO Secure Network Analytics Deployment \[pdf\]](#)
Instruction Manual
Secure Network Analytics Deployment, Network Analytics Deployment, A
nalytics Deployment, Deployment

References

- [User Manual](#)

—Previous Post

Cisco Smart Software Licensing Owner’s Manual

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search

[Manuals+](#) | [Upload](#) | [Deep Search](#) | [Privacy Policy](#) | [@manuals.plus](#) | [YouTube](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.