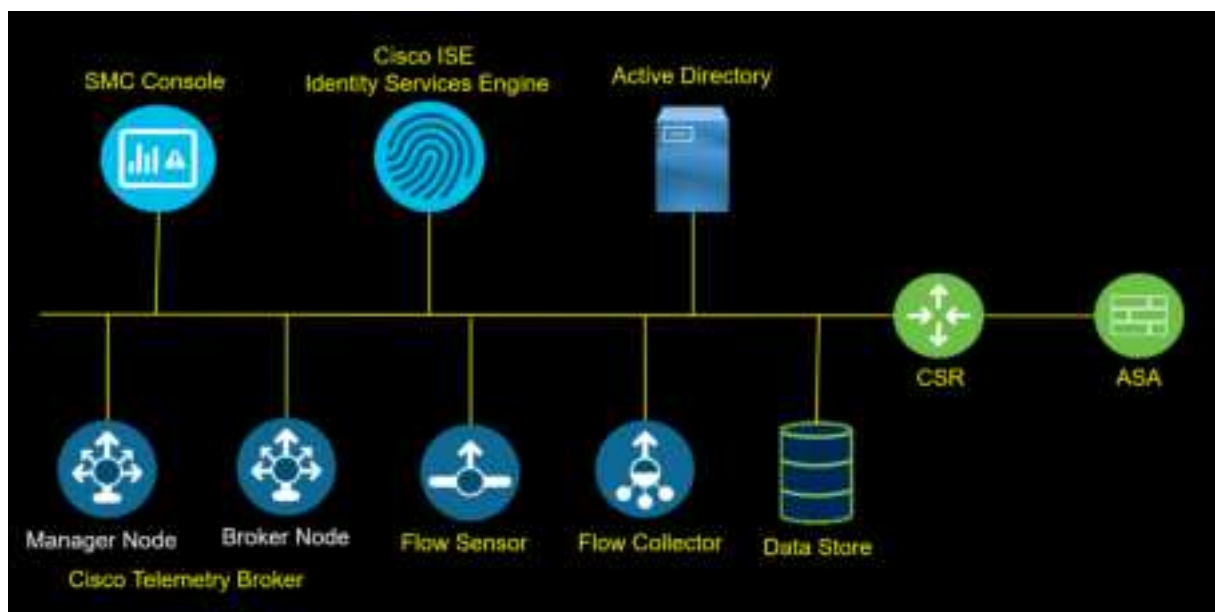


Cisco Secure Network Analytics Deployment and Cisco ISE Integration for ANC

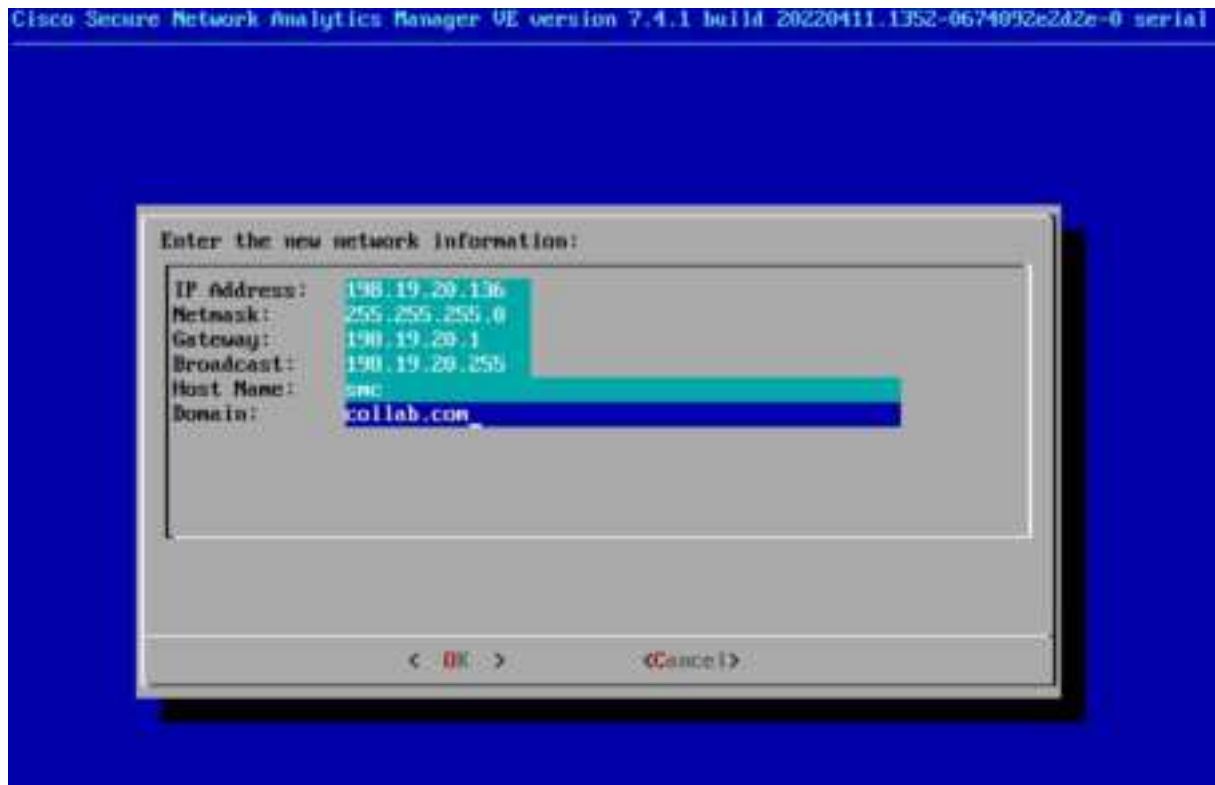


Redouane MEDDANE

Installation of SMC

Log in to the console, type the command **SystemConfig**.

Enter the network configuration for the appliance.



```

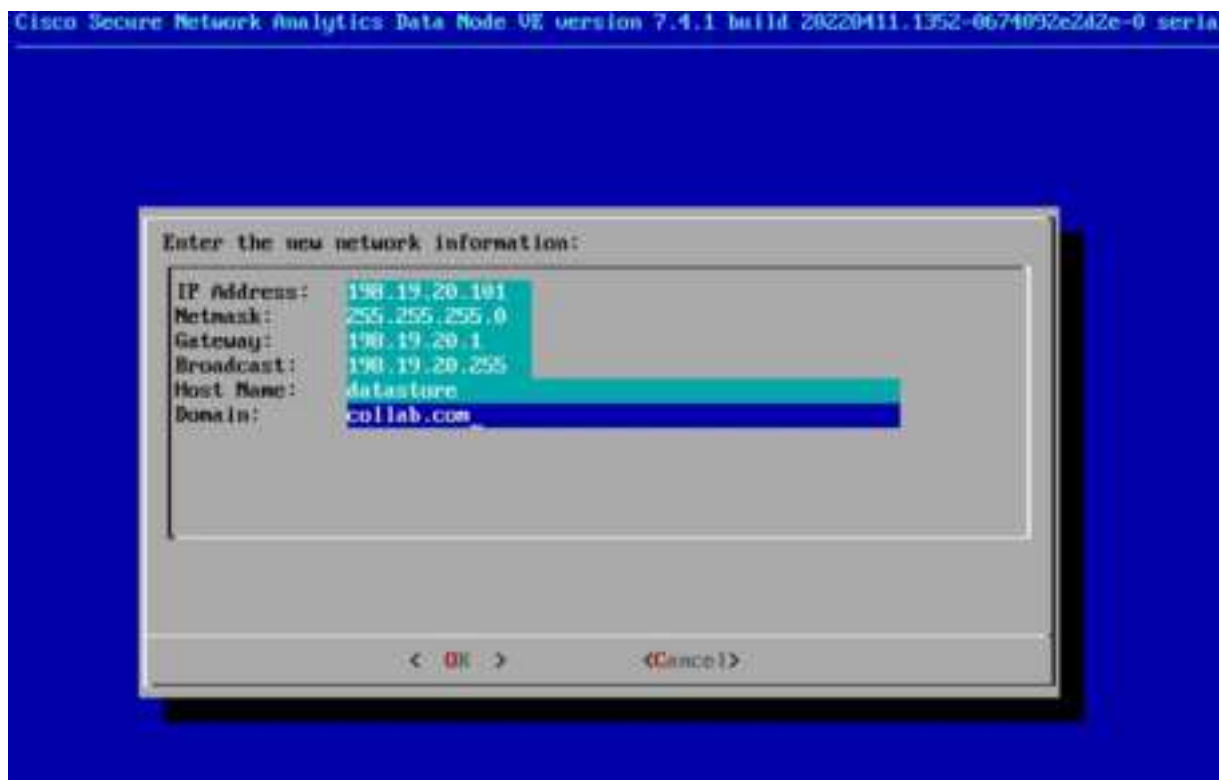
OK 1 Stopped Vertica Monitoring Service.
OK 1 Stopped irqbalance daemon.
OK 1 Removed slice system-getty.slice.
OK 1 Stopped LSB: Initialize EDDC.
OK 1 Stopped target System Time Synchronized.
OK 1 Stopped LSB: Start some power management scripts.
OK 1 Stopped LVM event activation on device 8:4.
OK 1 Removed slice system-lvm2\x2dposcan.slice.
OK 1 Stopped LSB: Start pdnsd.
OK 1 Stopped Session 14 of user root.
...
Stopping User Manager for UID 0...
Stopping Login Service...
OK 1 Unmounted Persistent Journal Storage.
OK 1 Stopped User Manager for UID 0.
Stopping User Runtime Directory /run/user/0...
OK 1 Unmounted /run/user/0.
OK 1 Stopped Availability of block devices.
OK 1 Stopped User Runtime Directory /run/user/0.
OK 1 Removed slice User Slice of UID 0.
Stopping D-Bus System Message Bus...
Stopping Permit User Sessions...
OK 1 Stopped LSB: set CPUfreq kernel parameters.

```

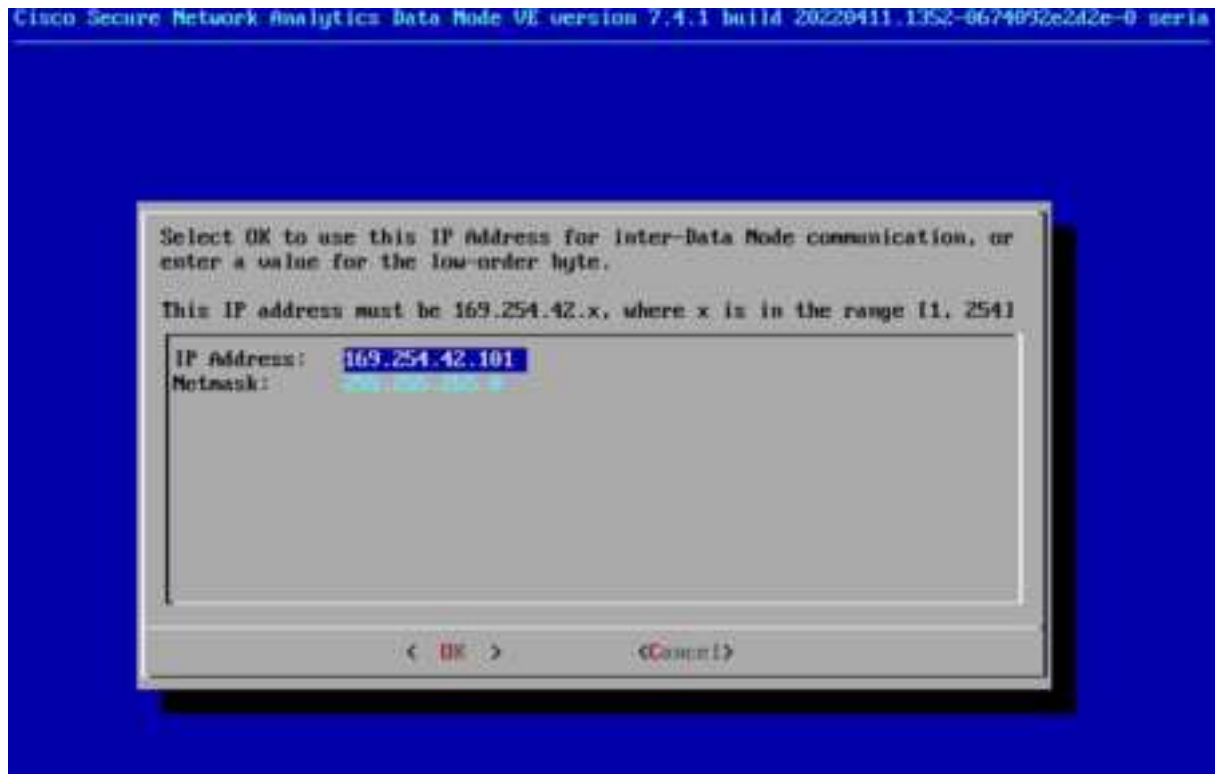
Installation of Datastore Node

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

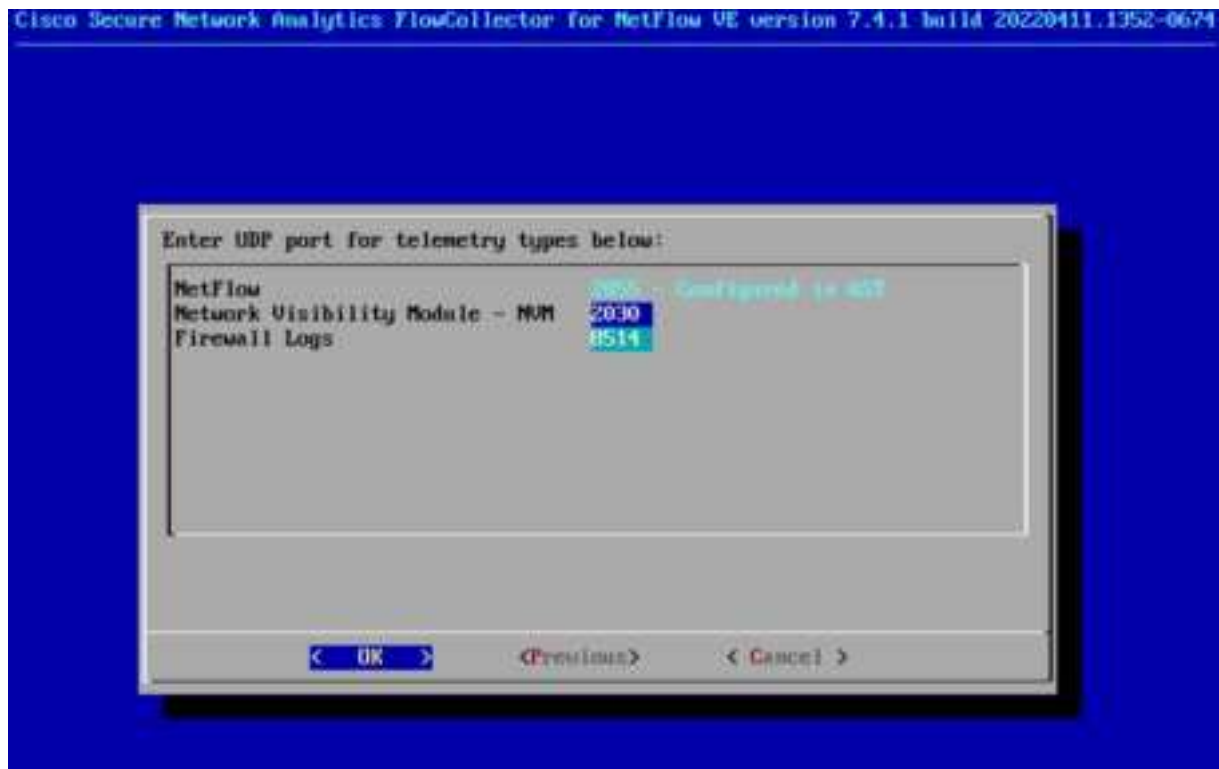
Log in to the console, type the command **SystemConfig**.

Ensure that all telemetry options are selected.

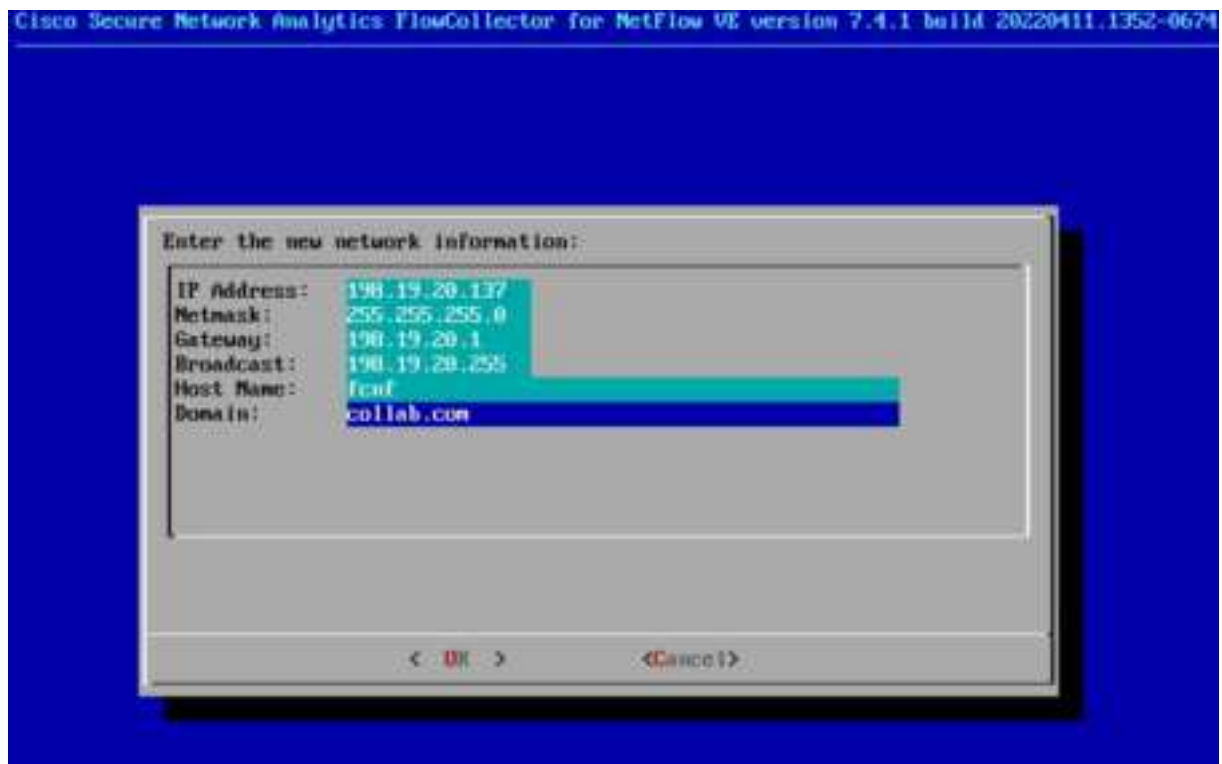


Configure the ports for the telemetry.

- 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 command **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 powerful 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 different 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.



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.



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



Step 1:
Change Default Password

Step 2:
Management Network Interface

Step 3:
Host Name and Domain

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 255 characters
- Must be different from the previous password by at least 4 characters
- Must not be the same as the previous 10 passwords(s)
- Must not be similar to the name of your appliance
- Must include 36 binary 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

Back

Next

Step 1:
Change Default Password

Step 2:
Management Network Interface

Step 3:
Host Name and Domain

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 255 characters
- Must be different from the previous password by at least 4 characters
- Must not be the same as the previous 10 passwords(s)
- Must not be similar to the name of your appliance
- Must include 36 binary 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

Back

Next

Step 1: Change Default Password

Step 2: Management Network Interface

Step 3: Host Name and Domain

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 passwords
- Must not be same as the same as any username
- Must include uppercase words and numbers or whitespace 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:

Back

Next

No changes for the Management Network Interface.

Step 1: Change Default Password

Step 2: Management Network Interface

Step 3: Host Name and Domain

Step 4: DNS Settings

Step 5: NTP Settings

Step 6: Register Your Appliance

Complete

Management Network Interface

Enable communication between the appliance and the network. Default network settings for the 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 silently substitutes a new IP address automatically. If you have a custom certificate, save the certificate and provide the path below you change. Have a backup you don't lose data.

Interface Name:

eth0

Interface MAC Address:

00:00:00:00:00:00

IPv4

IPv6

IP Address:

196.16.20.100

Subnet Mask:

255.255.255.0

Default Gateway:

196.16.20.1

Broadcast Address:

196.16.20.255

Back

Next

Configure the Host Name and Domains.

The screenshot shows a configuration page titled "Host Name and Domains". On the left is a vertical sidebar with a progress indicator showing six steps: Step 1: Change Default Password, Step 2: Configure Network Interface, Step 3: Host Name and Domains (highlighted in orange), Step 4: DNS Settings, Step 5: NTP Settings, Step 6: Register Your Appliance, and a final "Complete" step with a green checkmark.

The main content area is titled "Host Name and Domains" and includes a sub-header: "Enter identifying information for this appliance and the network domain where it is installed." Below this is a warning box: "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 or you will lose data."

The configuration fields are as follows:

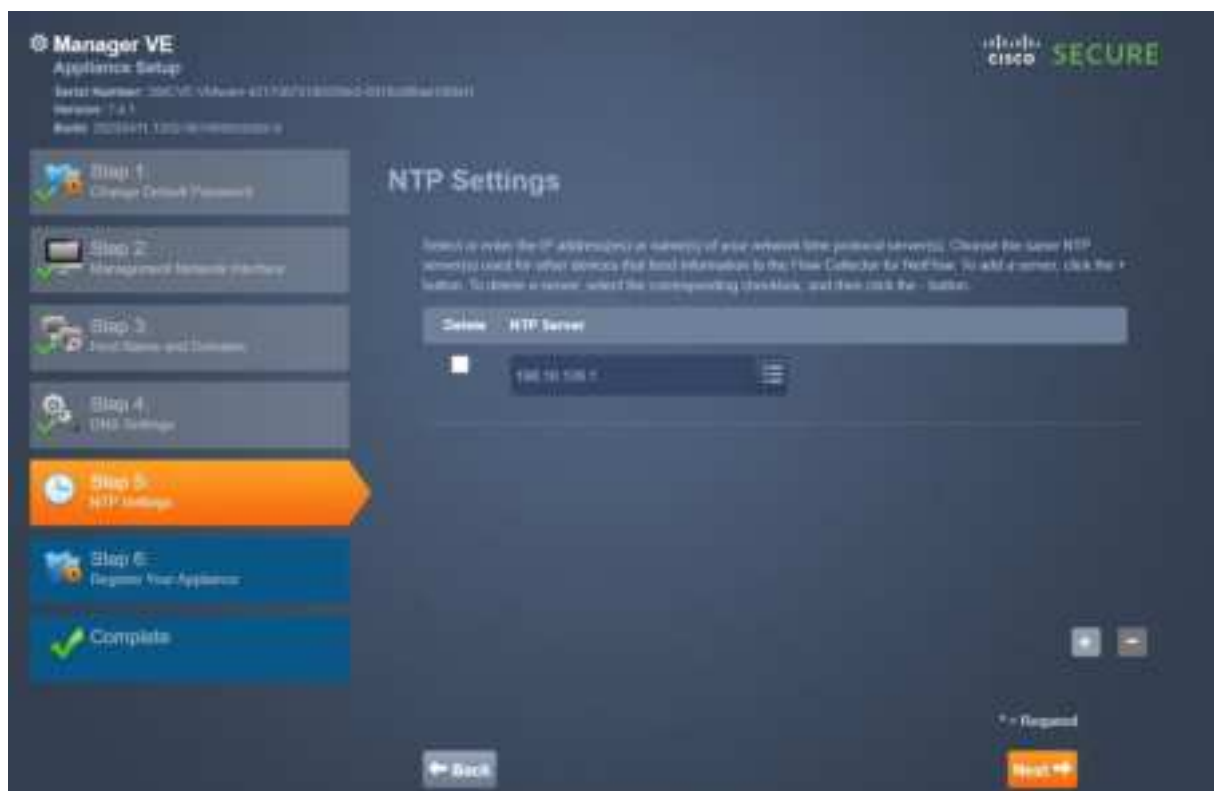
- Host Name:** A text input field containing "apc".
- Network Domain:** A text input field containing "csllab.com".
- Manager Domain:** A text input field containing "CCS.LAB".
- Manager Domain Type:** A dropdown menu currently set to "Data Store".
- IP Address Ranges:** A list box containing four IP ranges: "10.0.0.0/8", "192.168.0.0/16", "172.16.0.0/12", and "100.0.0.0/8".

At the bottom right, there is a "Back" button and a "Next" button (highlighted in orange).

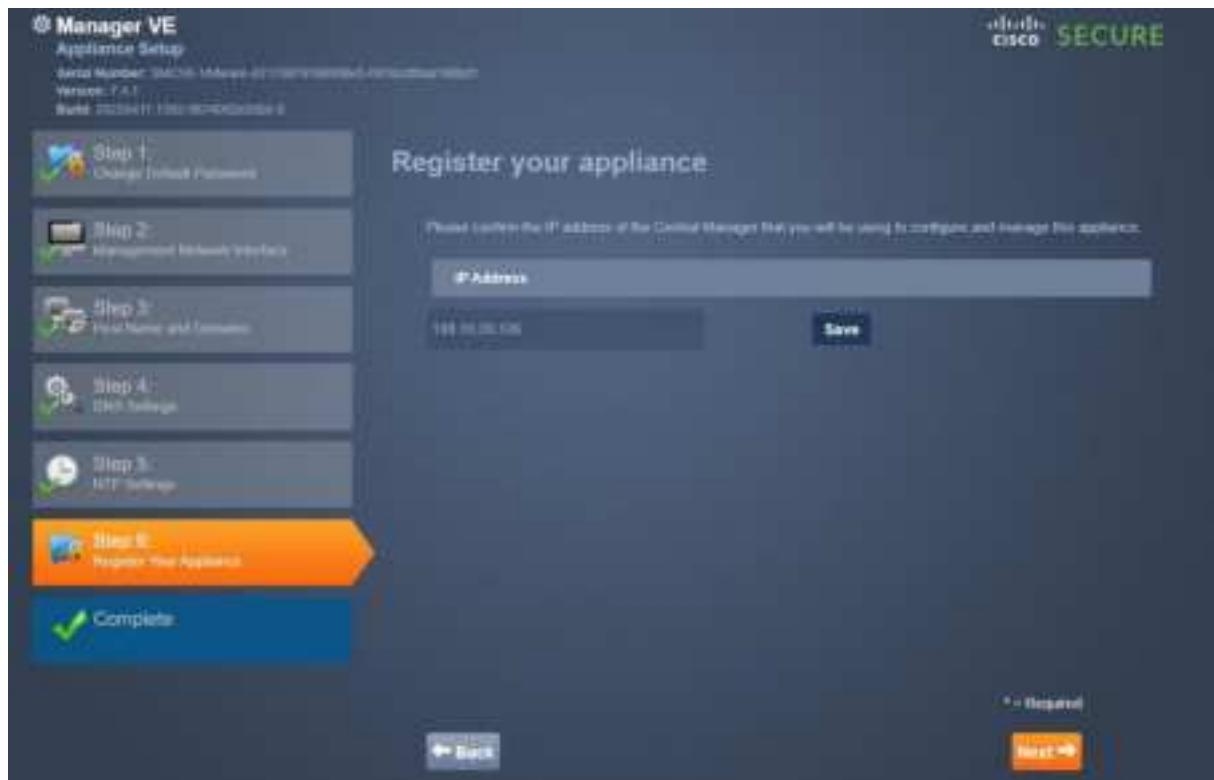
Configure the DNS Servers.



Configure the NTP Server.



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.



The screenshot shows the Cisco Central Management Inventory Table. The table has columns for Application Status, Application Name, Type, IP Address, and Actions. There are four rows of data, all with a status of 'Connected'.

Application Status	Application Name	Type	IP Address	Actions
Connected	Flow Collector	Flow Collector (SNA-FC)	198.19.20.137	...
Connected	Flow Collector	Flow Collector (SNA-FC)	198.19.20.137	...
Connected	Flow Collector	Flow Collector (SNA-FC)	198.19.20.137	...
Connected	Flow Collector	Flow Collector (SNA-FC)	198.19.20.137	...

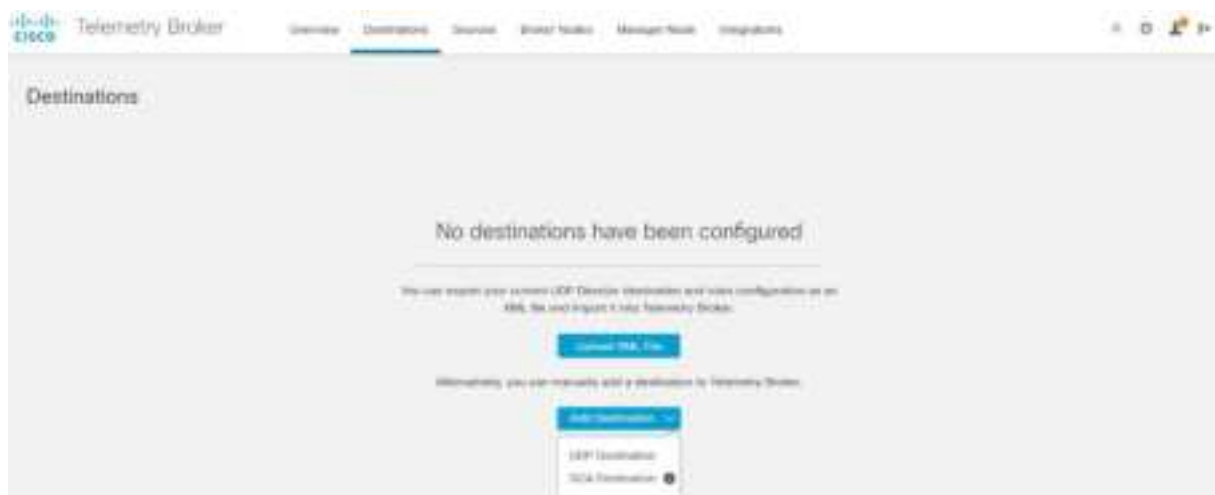
Cisco Telemetry Broker Configuration

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





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**.



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



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**.

The screenshot shows the 'Generate a CSR' form in the Cisco ISE GUI. The form is titled 'Generate a CSR' and has a 'Generate CSR' button. It contains several fields for generating a Certificate Signing Request (CSR). The fields are organized into two columns. The left column includes 'Add new length', 'Organization', 'Security ID', 'Security ID type', 'Key size', 'Security Code', and 'Key'. The right column includes 'Certificate type', 'Organization unit', 'Security Attribute', 'State or Province', 'Country', and 'Email Address'. The 'Generate CSR' button is located at the bottom right of the form.

The screenshot shows the 'Additional SSL/TLS Client Information' form in the Cisco ISE GUI. The form is titled 'Additional SSL/TLS Client Information' and has a 'Download CSR' button. It contains several fields for providing additional information for the CSR. The fields are organized into two columns. The left column includes 'Add SSL/TLS Client Identity', 'Identity Name', and 'Identity Type'. The right column includes 'Certificate Type', 'Certificate Format', and 'Certificate Password'. The 'Download CSR' button is located at the bottom right of the form.

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**

Generate pxGrid Certificate

Generating a single certificate with certificate signing request

Certificate Signing Request Details

Certificate Name: pxgrid-cert

Certificate Owner: pxgrid-cert

Expiration Date (YYYY-MM-DD): 2025-12-31-12

Certificate Format: PKCS12 (Exportable Certificate Chain - use for the public key certificate only)

Certificate Request: -----

Certificate Response: -----

Generate **Cancel**

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

Note :

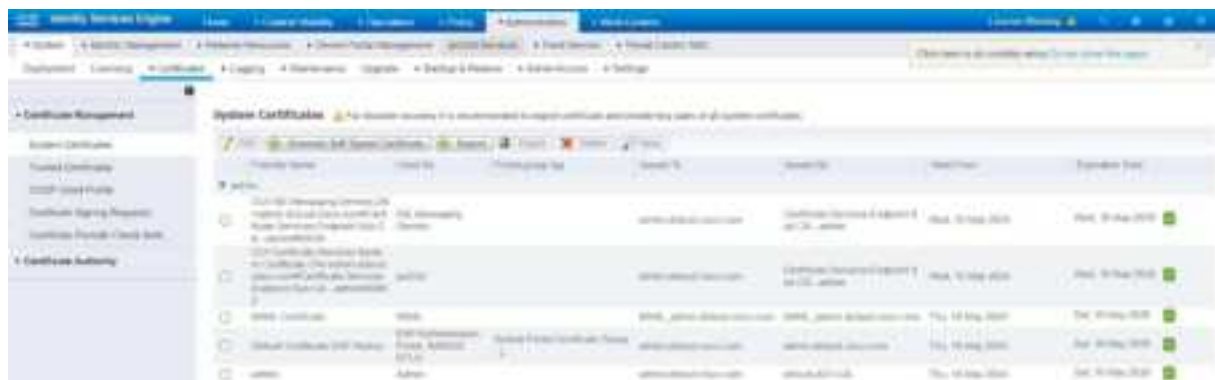
In some existing Cisco ISE deployment, you may have expired system certificates used for admin, eap and pxGrid services as shown below.

Certificate Name	Status	Issued To	Issued By	Issued On	Expiration Date	Expiration Status
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired

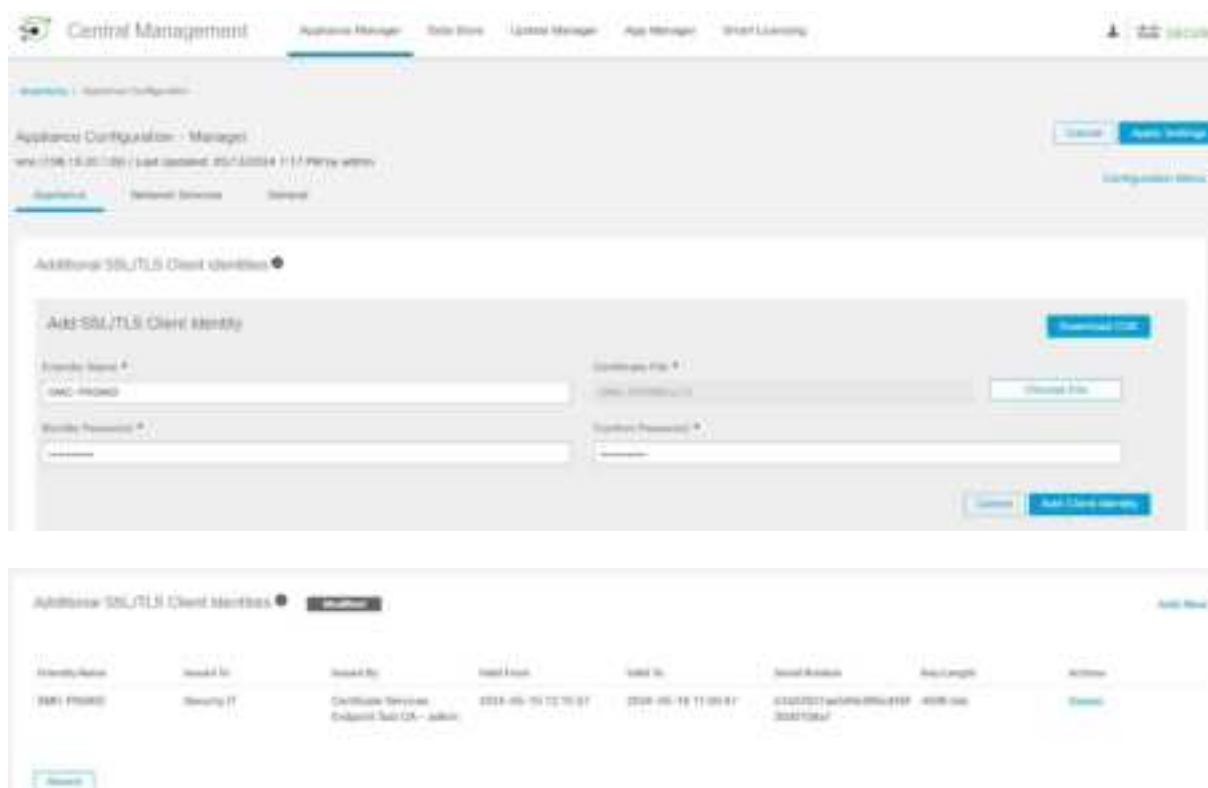
This is because the Cisco ISE internal CA certificates that sign these system certificates are expired.

Certificate Name	Status	Issued To	Issued By	Issued On	Expiration Date	Expiration Status
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired
Certificate Services Root (CA - pxgrid-cert)	Expired	Internal Services (Internal Services)	Internal Services (Internal Services)	2025-12-31-12-00-00	2025-12-31-12-00-00	Expired

In the **Usage** field, select **ISE Root CA**, then click on **Replace ISE Root CA Certificate Chain**.



Access the SMC GUI. Go to **Central Management**. In the SMC **Appliance Configuration** tab, scroll down to **Add SSL/TLS Client Identity** form, then click Choose File, select the **SMC-PXGRID** certificate.



The screenshot shows the SMC GUI interface. The top navigation bar includes 'Central Management', 'Appliance Manager', 'Data Store', 'Update Manager', 'App Manager', and 'Smart Licensing'. The main content area is titled 'Appliance Configuration - Manager' and shows the 'Additional SSL/TLS Client identities' section. The 'Add SSL/TLS Client Identity' form is visible, with fields for 'Identity Name' (SMC-PXGRID), 'Certificate File' (SMC-PXGRID.cer), 'Private Key' (SMC-PXGRID.key), and 'Certificate Password' (SMC-PXGRID). The 'Add SSL/TLS Client Identity' button is highlighted. Below the form, a table lists the added identities.

Identity Name	Issued To	Issued By	Issued From	Issued To	Serial Number	Key Length	Actions
SMC-PXGRID	Security IT	Certificate Services Endpoint Auto CA - Admin	2024-05-19 12:10:57	2024-05-19 12:10:57	0320702146546489495F-4038-040-3048708a7	4096 bits	Export

In the SMC GUI, navigate to **Deploy > Cisco ISE Configuration**.

Configure the ISE Configuration with the following parameters:

- Cluster Name: ISE-CLUSTER
- Certificate: SMC-PXGRID
- Primary PxGrid Node: 198.19.20.141
- Client Name: SMC-PXGRID

Network Analytics [Home](#) [Settings](#) [Dashboard](#) [Monitor](#) [Analyze](#) [Jobs](#) [Configure](#) [Export](#)

Cisco ISE Configuration Setup

Connection Details

Cluster Name:

Cluster ID:

Primary Node 1:

Primary Node 2:

Primary Node 3:

Client Name:

Integration options

Integrated Product:

- ☒ Cisco ISE
- ☐ Cisco ISE PC-Anywhere Security Connector

☐ Adaptive Network Control

☐ Cisco ISE Classification

☐ Discovery

☐ Track sessions started from multiple authentications

[Cancel](#) [Save](#)

Network Analytics [Home](#) [Settings](#) [Dashboard](#) [Monitor](#) [Analyze](#) [Jobs](#) [Configure](#) [Export](#)

Cisco ISE Configuration

[View configuration](#)

Cluster Name	Cluster ID	Primary Node 1	Primary Node 2	Primary Node 3	Client Name
ISE-Cluster	ISE-Cluster	192.168.1.1	192.168.1.2	192.168.1.3	ISE-Cluster

Network Analytics [Home](#) [Settings](#) [Dashboard](#) [Monitor](#) [Analyze](#) [Jobs](#) [Configure](#) [Export](#)

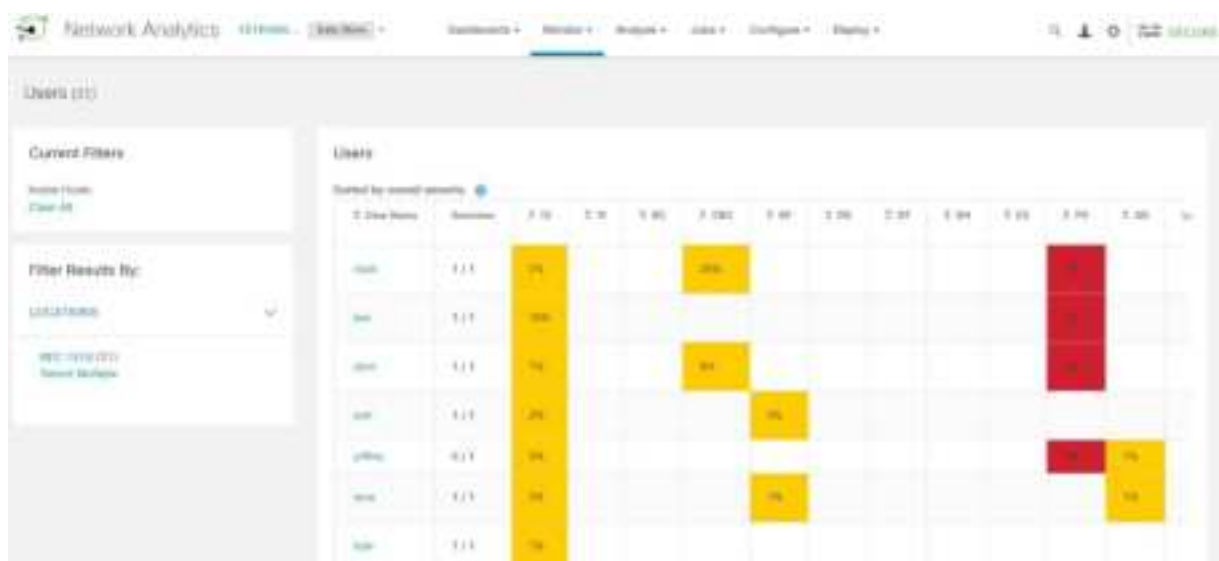
Cisco ISE Configuration

[View configuration](#)

Cluster Name	Cluster ID	Primary Node 1	Primary Node 2	Primary Node 3	Client Name
ISE-Cluster	ISE-Cluster	192.168.1.1	192.168.1.2	192.168.1.3	ISE-Cluster

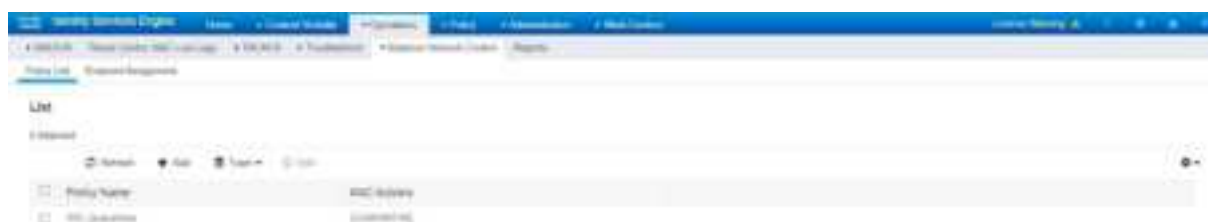
Navigate to **Monitor > Users**.

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.



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.

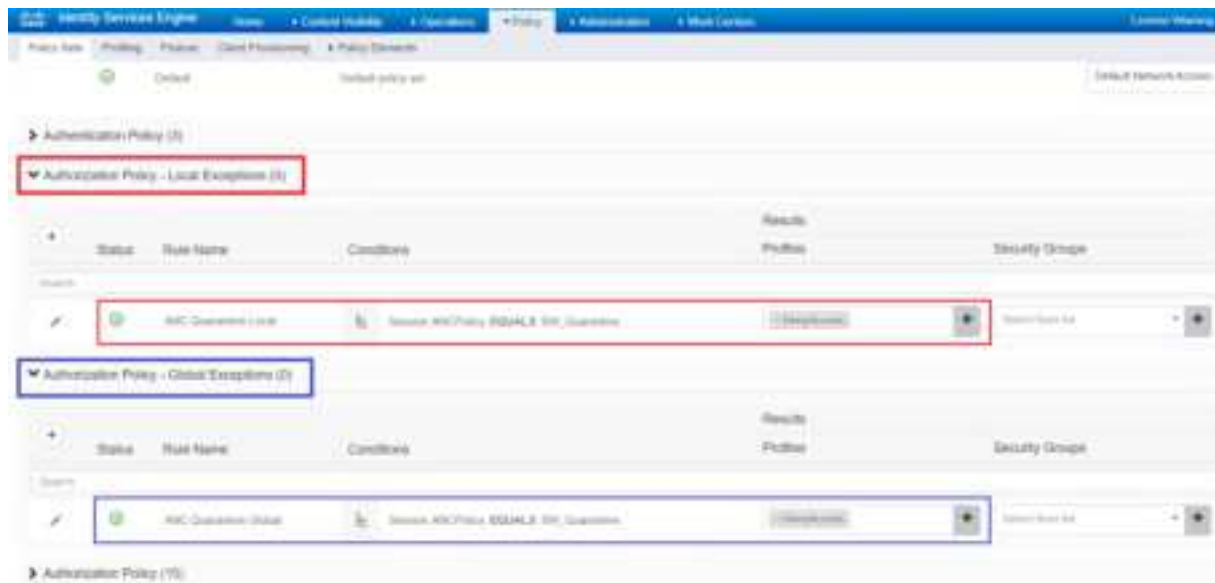
The local authorization exception rule overwrites the global exception rules. So the local exception rule is processed first, then the global exception rule, and finally, the normal rule of the authorization policy.

One of the interesting use case of these Exception Rules is when you configure Cisco Secure Network Analytics (Stealthwatch) with Cisco ISE for Response Management using Adaptive Network Policy (ANC) so that when an alarm is raised, Cisco Secure Network Analytics (Stealthwatch) will request Cisco ISE to quarantine the host with Adaptive Network Control Policy through PxGrid.

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.



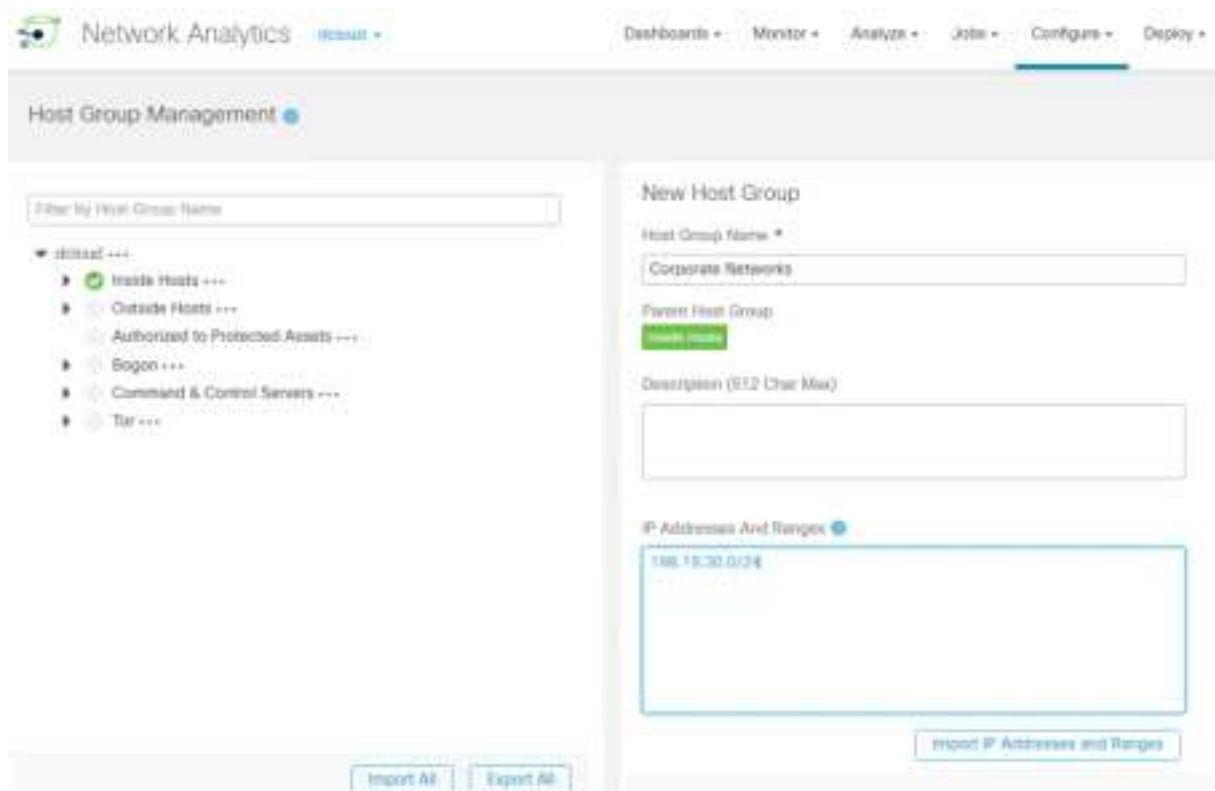
Automatic Action and Response with ANC

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.

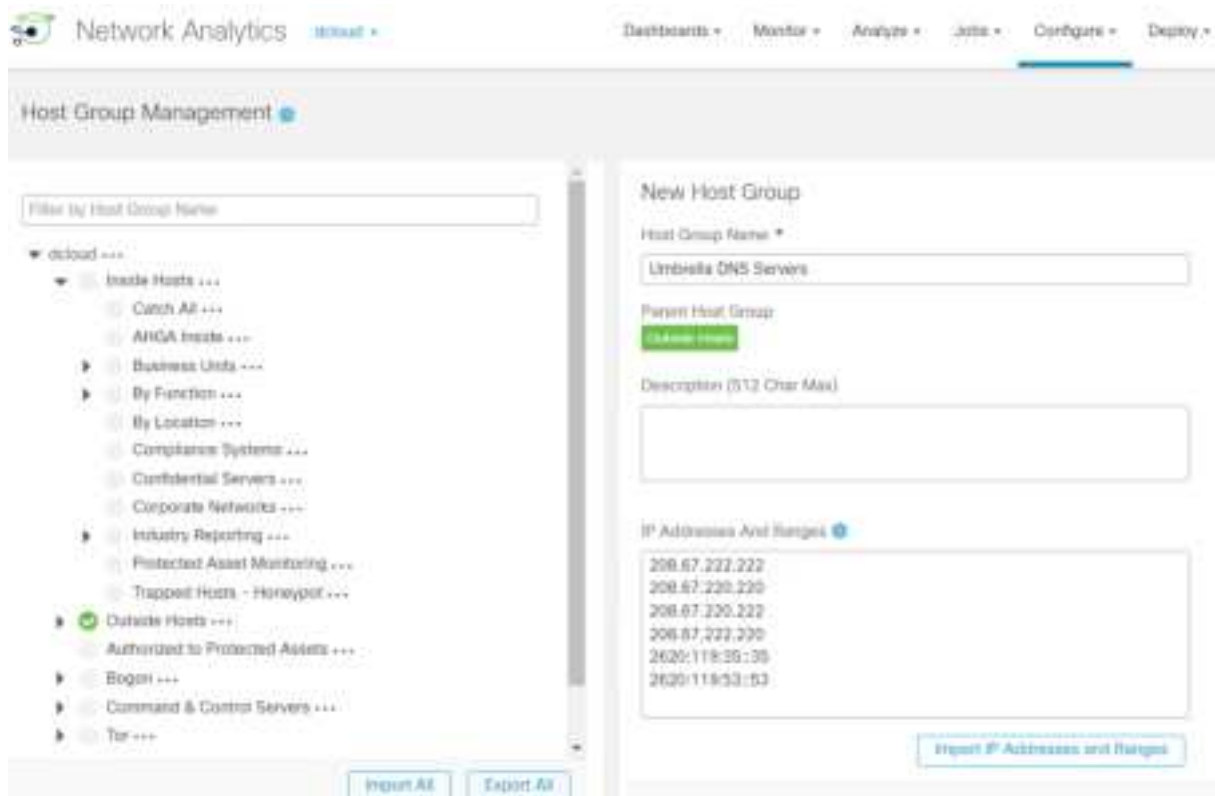
When an alarm is raised, Cisco Secure Network Analytics will request Cisco ISE to quarantine the host that uses rogue DNS Servers with Adaptive Network Control Policy through PxGrid.

Navigate to **Configure > Host Management**.

In the parent host group **Inside Hosts**, create a Host Group named **Corporate Networks** for your internal networks.



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



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

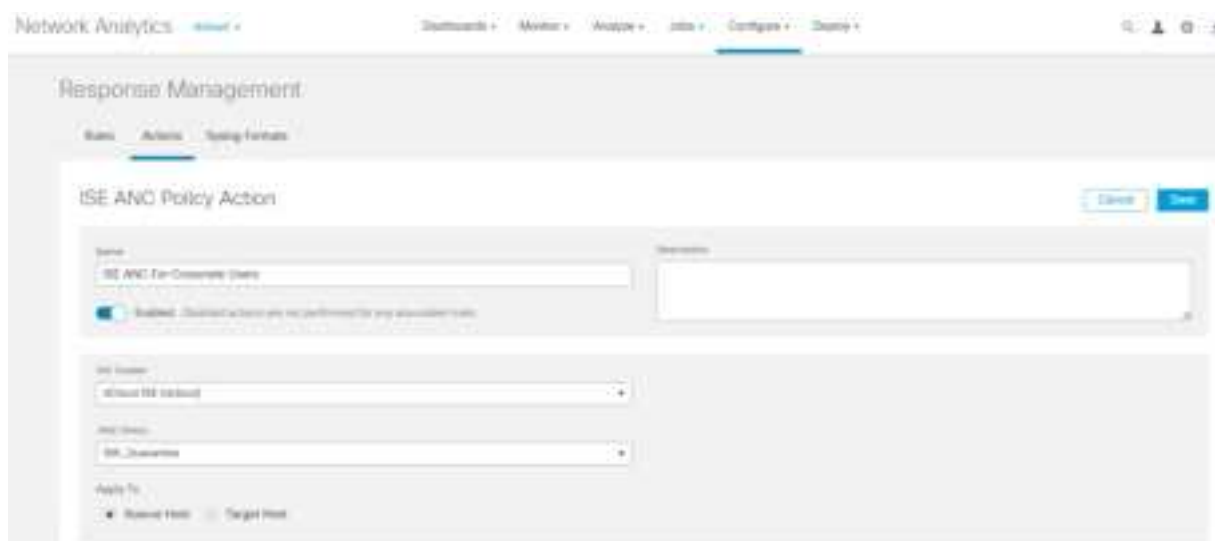
Basically this event is triggered when any host withing **Corporate Networks** Host Group communicates with any host within **Outside Hosts** Host Group except those within **Umbrella DNS Servers** Host Group, through 53/UDP or 53/TCP, an alarm is raised.



Navigate to **Configure > Response Management**. Click on **Actions**.



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.



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: Description:

☒ Enabled: Triggered when we see suspicious data when associated conditions are met

Rule is triggered if:

or the following is true

Associated Actions

Execute the following actions when the alert becomes active

Name	Type	Description	Used By Rules	Assigned
Auto Correlate with Cisco ISE ANC	ISE ANC Policy	Automatically generate the offending event or event message in ISE ANC policy action	1	<input type="checkbox"/>
ISE ANC for Corporate Data	ISE ANC Policy		0	<input checked="" type="checkbox"/>
Investigate	Event	Search for event by this category displayed in the Investigation tool. 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
          wwds.cisco.com.edgekey.net
          wwds.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:fd00:562::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.



Host IP Address	ISE Cluster	ISE Address	Assignment Mode	Requested By	Time	Requested ISE Policy	Effective ISE Policy	Assign ISE Policy
10.10.30.36	ISE-Cluster		Automatic	Request Management	2020-03-10 10:44	ISE_Quarantine	ISE_Quarantine	xxx