CISCO VALIDATED DESIGN

Network as a Sensor—Unified Wired-Wireless Deployment Guide

August 2016

REFERENCE
NETWORK
ARCHITECTURE

Table of Contents

Introduction 1

Cisco Network as a Sensor 1

Components at a Glance 2

Retail Use Case 5

Business Problem 5

Solution 7

HealthCare Use Case 9

Business Problem 9

Solution 10

Finance Use Case 11

Business Problem 11

Solution 12

Design Overview 13

Deployment Details 14

Deploying Cisco ISE (pxGrid) 16

Deploying Cisco Stealthwatch 26

Integrating Cisco ISE with Cisco Stealthwatch 31

Enabling NetFlow on Network Devices 40

Configuring C3850 Converged Access Switch with Wired and Wireless Support 41

Configuring NetFlow on WLC 46

Quarantining SGT 51

Quarantining VLAN 54

Verifying and Testing 55

Appendix A: Product List 60

Introduction

This guide describes how to enable Cisco Network as a Sensor (NaaS) in campus/branch ("east-to-west") traffic for wired and wireless users and briefly covers how to contain an attack.

Cisco NaaS provides deeper visibility in your network by leveraging NetFlow on switches, routers and wireless LAN controllers (WLCs), and it can quarantine attacks, leveraging Cisco Identity Service Engine (ISE), Cisco Platform Exchange Grid (pxGrid), and Cisco Stealthwatch.

For more information, see Cisco Cyber Threat Defense and Cisco Rapid Threat Containment.

CISCO NETWORK AS A SENSOR

A network's attack surface is continually growing. Today's technology trends such as mobility, cloud, and the Internet of Things (IOT) are multiplying the points of infiltration into your network, and attackers are getting more sophisticated. Often attackers are part of international cybercrime organizations with monetary motivations, and the attackers may understand your network and defenses better than you do. Many times, they will use legitimate user credentials to accomplish their objectives. As a result, discovery and network remediation of the breaches are complex, time consuming, and extremely costly.

When addressing such a complex security problem, depending on a single hardware or software component is not the right approach. Rather than taking a Swiss army knife approach (a single tool for multipurpose), you need to take a toolbox approach instead, which can provide function-specific tools. The Cisco NaaS solution is a toolbox consisting of NetFlow, Cisco ISE, and Cisco Stealthwatch. These tools are tightly integrated to help you leverage the entire network in order to:

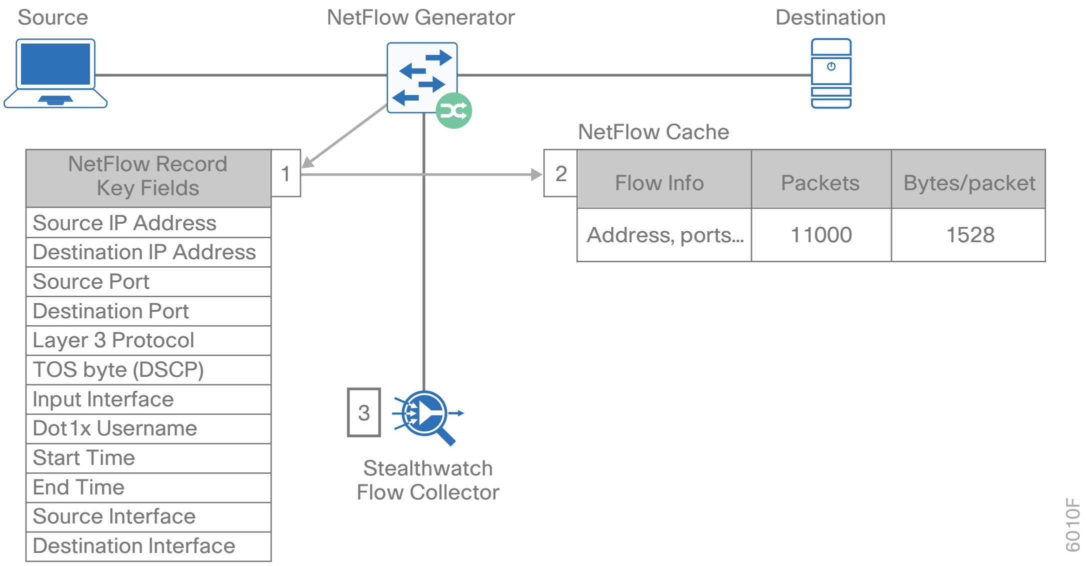
- Detect anomalous traffic flows such as malware.
- Identify user access policy violations.
- Obtain deep and broad visibility in to all network traffic.

COMPONENTS AT A GLANCE

NetFlow

NetFlow is a small package of metadata describing the "conversations" on the network. It contains the important details in network transactions' endpoints of data communication, information about when the conversation occurred, how long it lasted, and what protocols were used. It is a Layer 3 (possibly Layer 2, based on where it's enabled or match conditions) network protocol, which you can easily enable on wired and wireless devices for visibility into the network flows, as well as enhanced network anomaly and security detection.

Figure 1 *NetFlow operation on network device*



NetFlow Record Key Fields
Source IP Address
Destination IP Address
Source Port
Destination Port
Layer 3 Protocol
TOS byte (DSCP)
Input Interface
Dot1x Username
Start Time
End Time
Source Interface
Destination Interface

Flow Info	Packets	Bytes/packet
Address, ports...	11000	1528

For more information, see Cisco IOS NetFlow.

Cisco Identity Service Engine

Cisco ISE is a single policy-control-point for identity, access control, and device security across wired, wireless, and VPN networks. You can leverage ISE to determine additional network context for exported NetFlow from network devices. It's a threat-centric policy server that can exchange context via pxGrid and can mitigate threats in real-time and prevent their spread across the network.

For more information, see Cisco Identity Services Engine.

Cisco Platform Exchange Grid

Cisco Platform Exchange Grid (pxGrid) is part of Cisco ISE technology that allows sharing rich contextual data with other Cisco platforms, as well as integrated partner ecosystem solutions. This makes it easier than ever to add features to identify, mitigate, and remediate security threats across the network. Overall, secure access control is centralized and simplified to securely deliver vital business services, enhance infrastructure security, enforce compliance, and streamline service operations.

For more information, see Cisco Platform Exchange Grid.

Cisco TrustSec

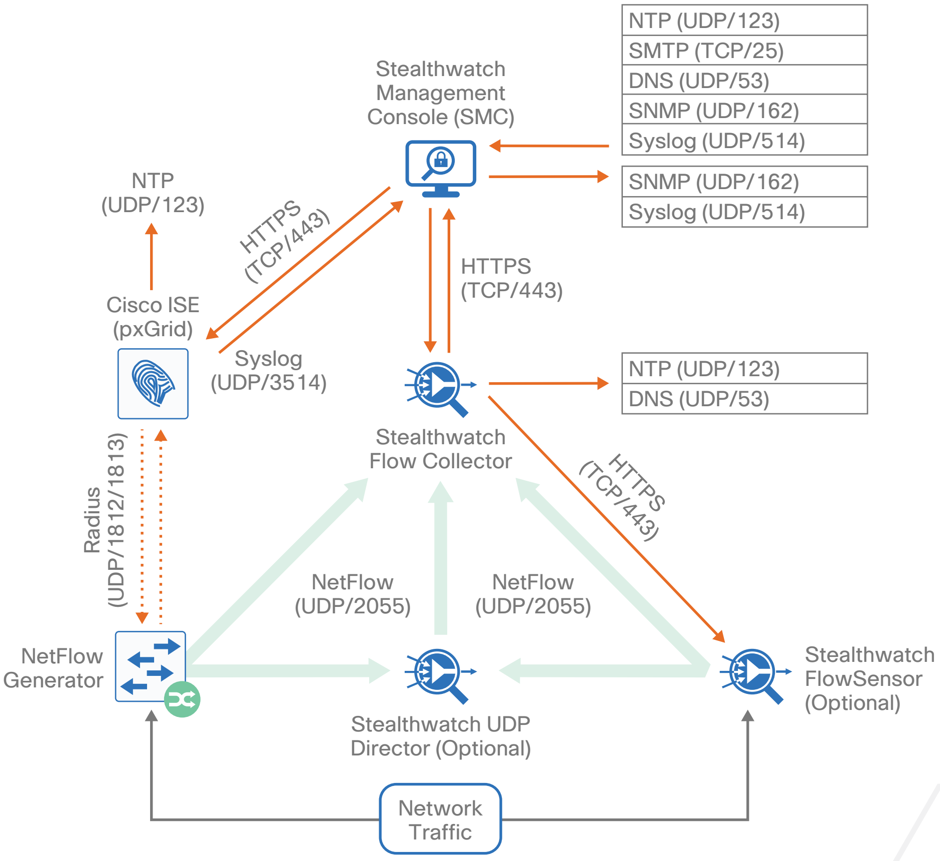
Combined with ISE, Cisco TrustSec can segment your network and enforce role-based, topology-independent, and access-independent access control by using software-defined segmentation—also known as Security Group Tags (SGT)—in order to simplify the provisioning and management.

For more information, see Cisco TrustSec.

Cisco Stealthwatch

Cisco Stealthwatch harnesses the power of NetFlow in order to provide advanced network visibility, security intelligence, analytics, and protection across the entire attack continuum (before, during, and after). This visibility allows a metadata record to be maintained for every communication that traverses a network device. You can analyze this aggregated data in order to identify hosts with suspicious patterns of activity. Stealthwatch has a specific *Reconnaissance* alarm category with several different algorithms watching behavior and identifying suspicious activity. It is basically leveraging NetFlow data from network devices throughout all layers of the network—access, distribution, core, and edge.

Figure 2 Data Flows with Stealthwatch



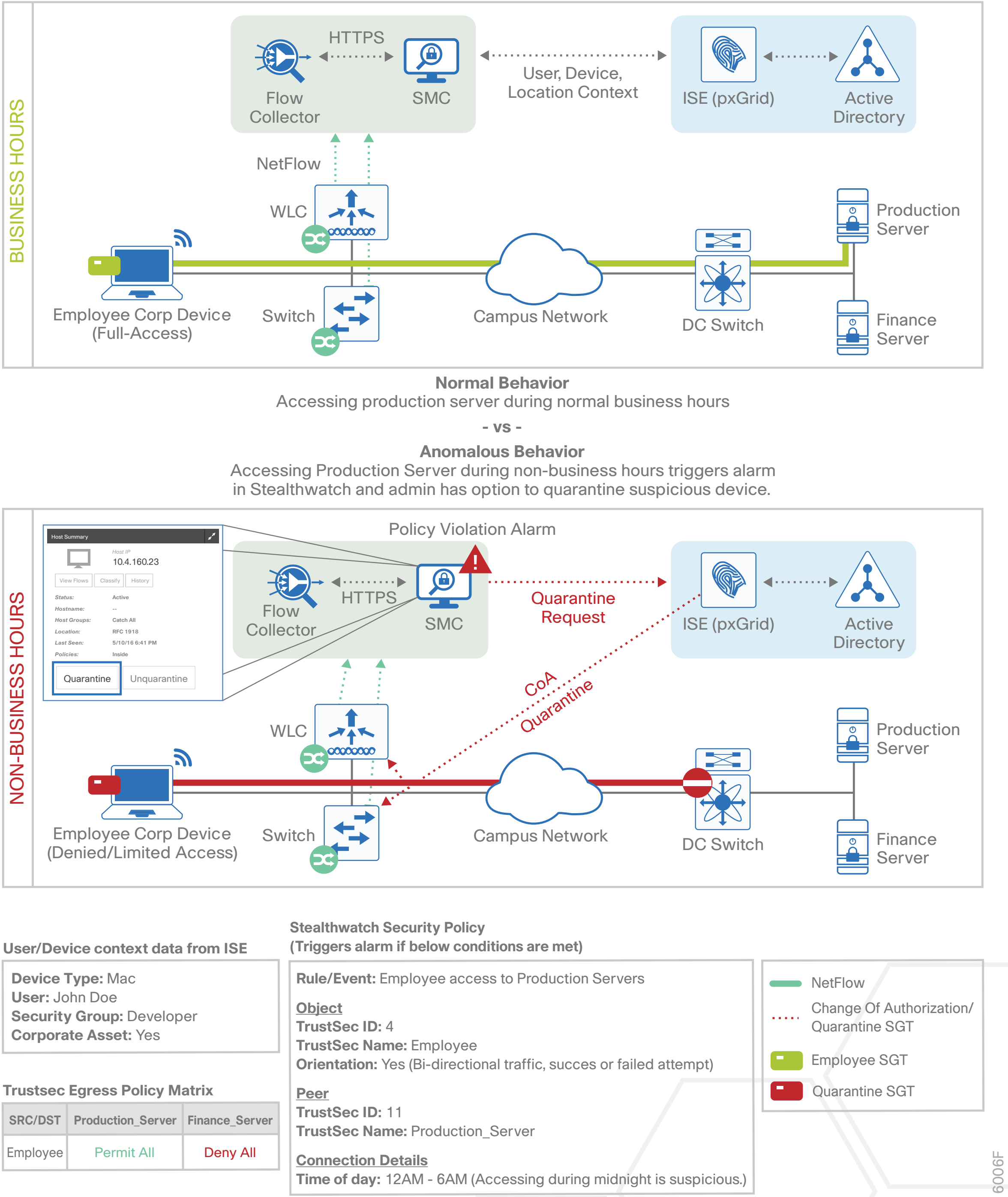
For more information, see Cisco Stealthwatch.

Network as a Sensor

You can transform your existing Cisco network infrastructure into a security sensor and monitoring system, giving you a powerful and scalable solution for gaining deep visibility (who, what, when, where, and how), control, and analytics of the network traffic by simply activating NetFlow.

For more information, see Network as a Sensor.

Figure 3 Typical NaaS topology in a branch/campus scenario



Normal Behavior
Accessing production server during normal business hours

- vs -

Anomalous Behavior
Accessing Production Server during non-business hours triggers alarm in Stealthwatch and admin has option to quarantine suspicious device.

Host Summary
Host IP 10.4.160.23
View Flows | Classify | History
Status: Active
Hostname: --
Host Groups: Catch All
Location: RFC 1918
Last Seen: 5/10/16 6:41 PM
Policies: Inside
Quarantine | Unquarantine

User/Device context data from ISE

Device Type: Mac
User: John Doe
Security Group: Developer
Corporate Asset: Yes

Trustsec Egress Policy Matrix

SRC/DST	Production_Server	Finance_Server
Employee	Permit All	Deny All

Stealthwatch Security Policy
(Triggers alarm if below conditions are met)

Rule/Event: Employee access to Production Servers

Object
TrustSec ID: 4
TrustSec Name: Employee
Orientation: Yes (Bi-directional traffic, succes or failed attempt)

Peer
TrustSec ID: 11
TrustSec Name: Production_Server

Connection Details
Time of day: 12AM - 6AM (Accessing during midnight is suspicious.)

🟩	NetFlow
⋯	Change Of Authorization/ Quarantine SGT
🟩	Employee SGT
🟥	Quarantine SGT

Retail Use Case

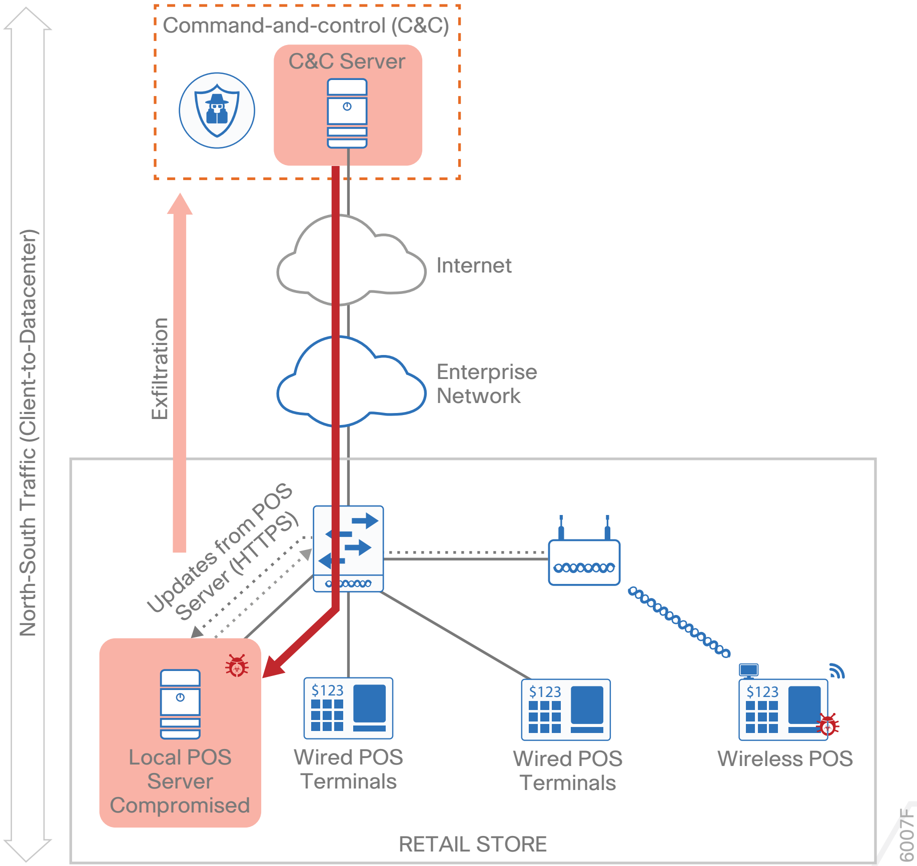
Retail stores have a credit card processing network. Normal behavior, then, is for the point-of-sale systems to communicate with a credit card processor, via HTTPS, sending the credit card transactions. These networks are very sensitive. As such, attackers love to get their hands on the traffic. This solution uses Stealthwatch to whitelist the expected network traffic and look for any new behaviors.

BUSINESS PROBLEM

If one of the point-of-sale (POS) terminals were compromised (maybe by malware, or maybe by someone plugging in a credit card skimmer), the network communications would change—such as the POS Terminal sending data to an unauthorized Command and Control server or infecting other endpoints by malware propagation.

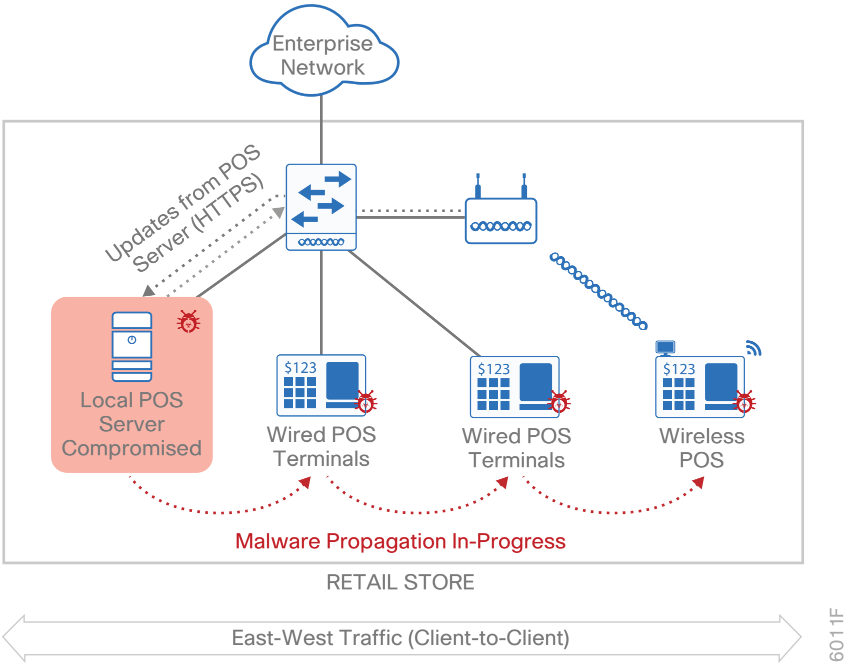
Example 1

The compromised local POS server starts sending (north-south) communications to an external malware Command and Control (C&C) server instead of the real payment server.



Example 2

The local POS server is compromised and starts propagating malware (east-west) to other POS terminals in the network.

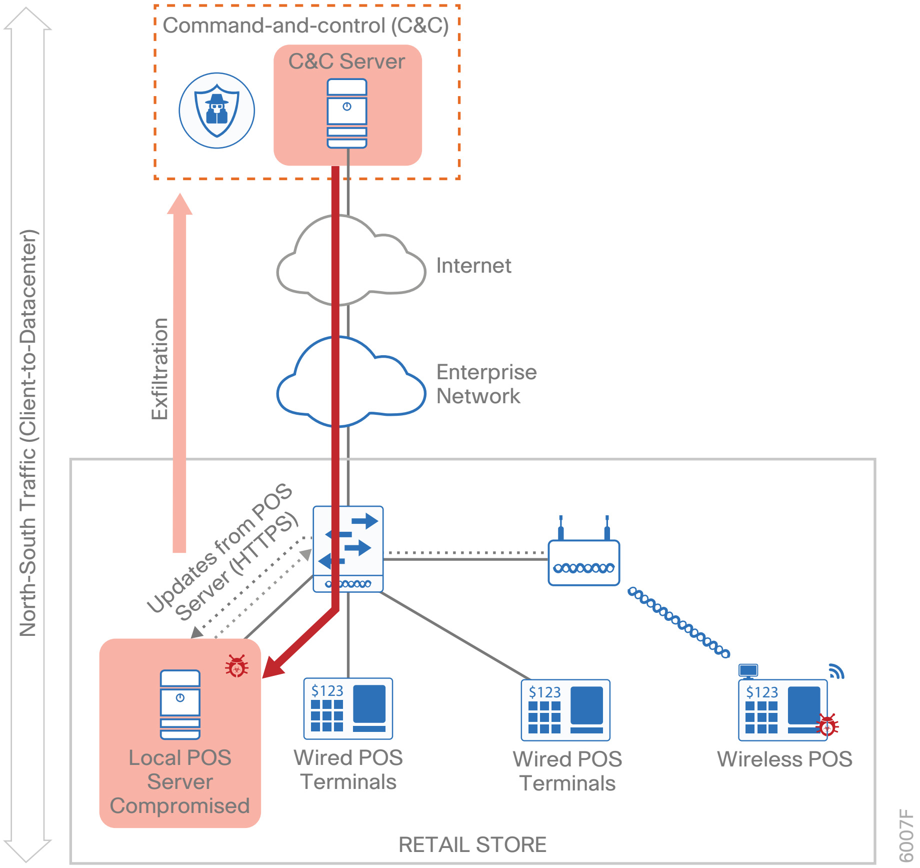

Enterprise Network
Updates from POS Server (HTTPS)
Local POS Server Compromised
$123
Wired POS Terminals
Wired POS Terminals
Wireless POS
Malware Propagation In-Progress
RETAIL STORE
East-West Traffic (Client-to-Client)
6011F

SOLUTION

Stealthwatch would see the change in network behavior and receives alerts on the dashboard about the anomalous behavior and identify the compromised systems, allowing the retail organization complete visibility into their network and to rapidly mitigate the compromise.

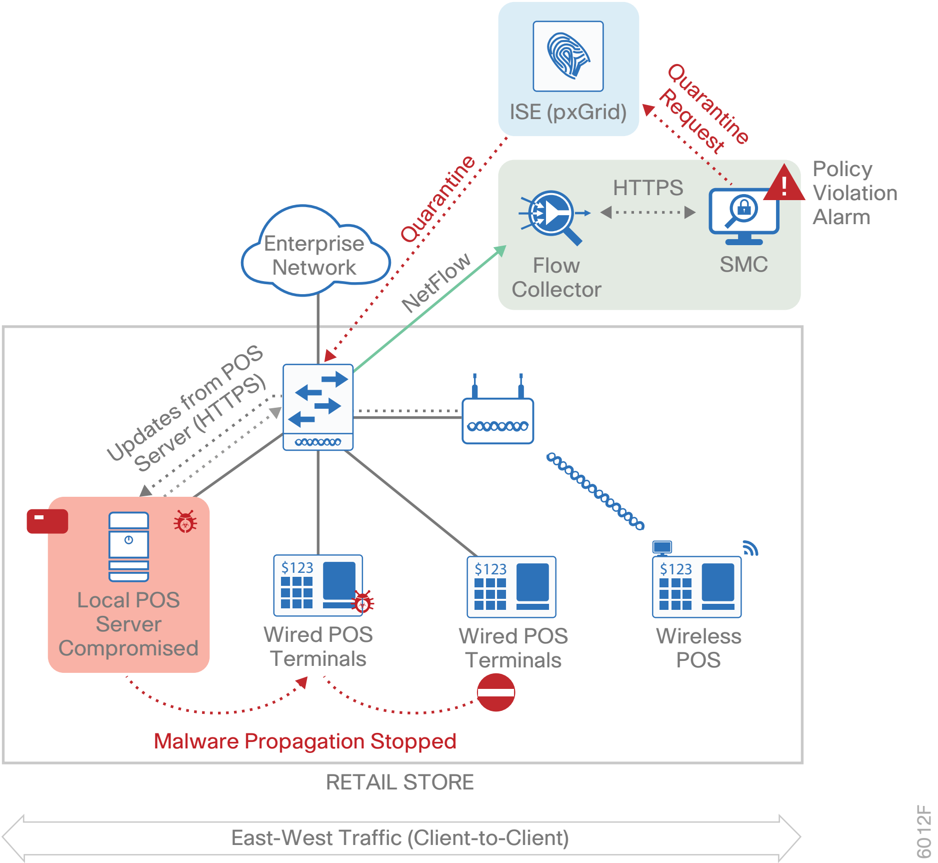
Example 1

When the compromised Local POS server starts sending (north-south) communications to an external malware C&C Server instead of the real payment server, enabling NetFlow on the switches or WLCs gives deeper visibility into the network with Stealthwatch, and it can flag that activity and alert the anomalous behavior. This will allow the admin to further investigate and quarantine a compromised user or device.



Example 2

As the compromised local POS server commands a POS terminal to start propagating malware to other POS terminals, in a NetFlow-enabled network, Stealthwatch can flag this activity and alert it as an anomalous behavior, because communication between the POS terminals is not normal behavior. This will allow the admin to further investigate and quarantine a compromised user or device.

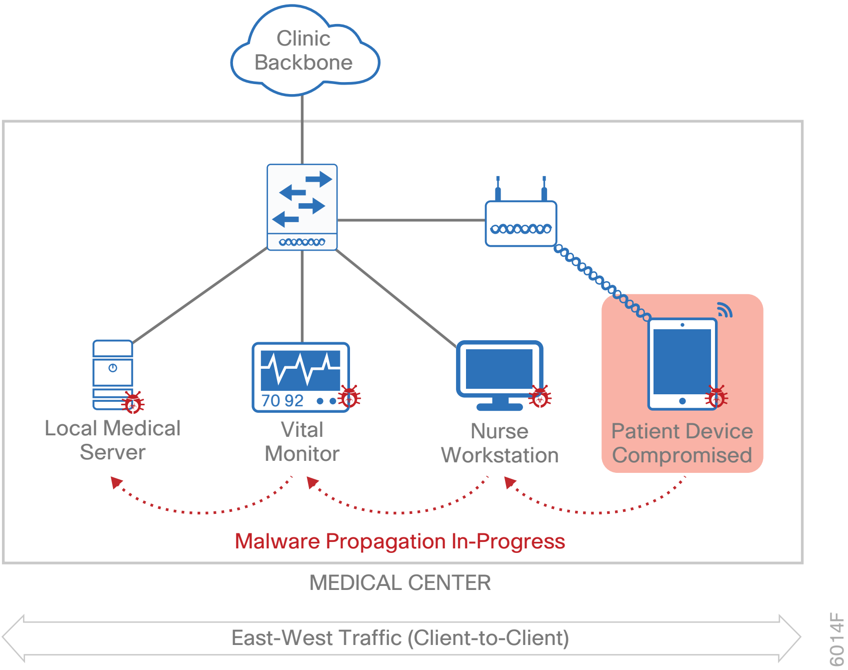


HealthCare Use Case

Our healthcare records are just as valuable to attackers as our credit card numbers and online passwords. In the wake of recent cyberattacks, hospitals are required to have HIPAA-compliant wired and wireless networks that can provide complete and constant visibility in to their network traffic in order to protect sensitive medical devices (such as electronic medical records servers, vital monitors or nurse workstations) so that a malicious device cannot compromise the networks.

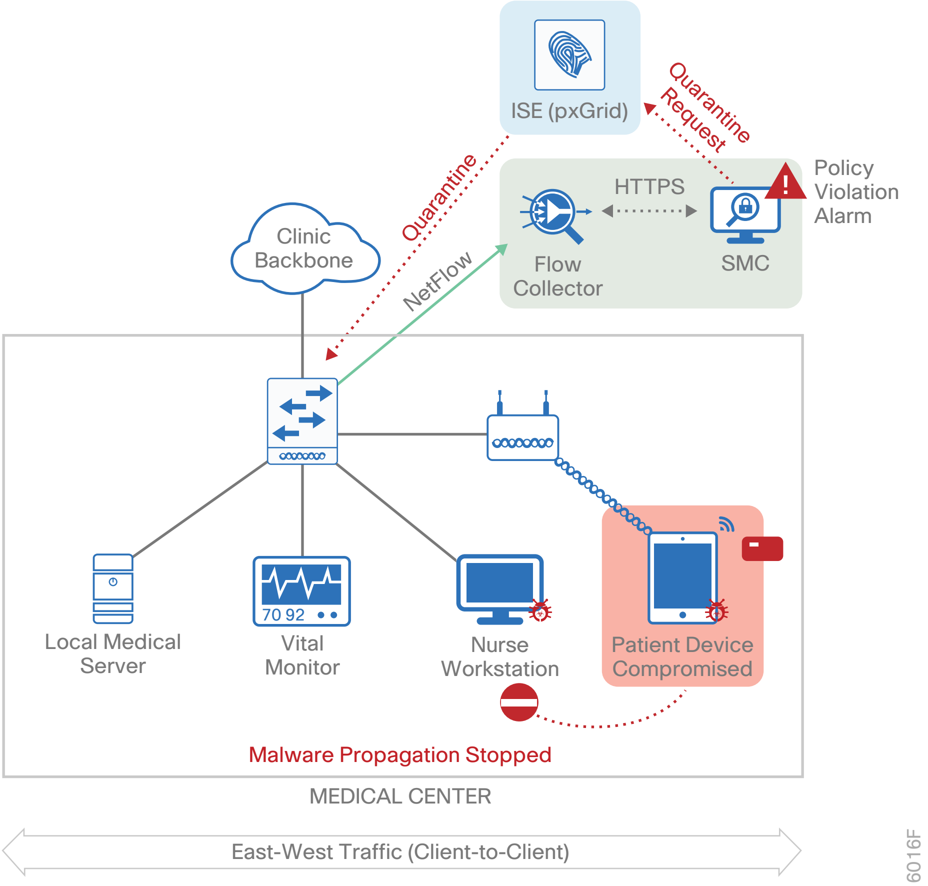
BUSINESS PROBLEM

A patient's mobile device is compromised by malware, and the network communication changes, infecting other endpoints by malware propagation (east-west).


Clinic Backbone
Local Medical Server
70 92
Vital Monitor
Nurse Workstation
Patient Device Compromised
Malware Propagation In-Progress
MEDICAL CENTER
East-West Traffic (Client-to-Client)
6014F

SOLUTION

When a patient's mobile device starts communicating with any medical devices, it's considered an abnormal behavior, whether the attempt is successful or not. Enabling NetFlow on the switches or WLCs gives deeper visibility into the network traffic behavior with Stealthwatch, and it can flag the unusual activity and alert as an anomalous behavior in SMC dashboard. This will allow the admin to further investigate and quarantine a compromised device with a single click.



Finance Use Case

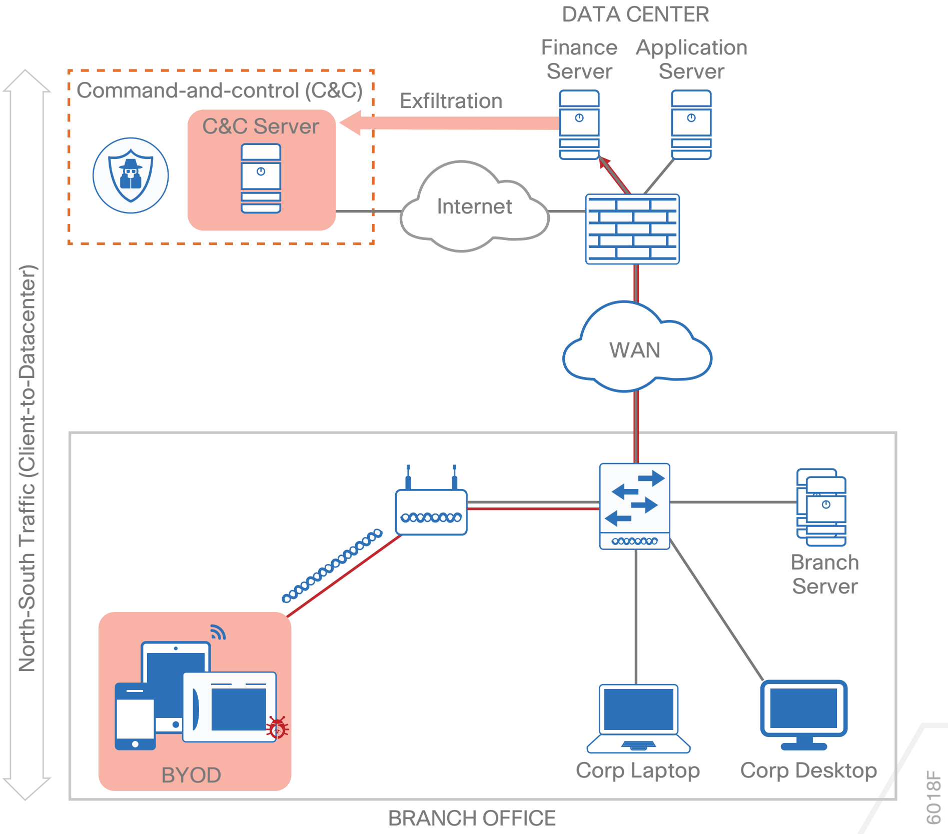
In an increasingly open network environment, financial institutions must:

- Protect the confidentiality, integrity, and availability of networks, applications, and data per regulatory and industry requirements.
- Define strict standards for network availability and security best practices—and stiff penalties for failure to meet or prove compliance with those standards.
- Provide customers and employees with 24/7 availability to critical financial information, without tolerating security breaches or unexpected interruptions in service.

BUSINESS PROBLEM

An employee at a financial institution uses his personal mobile device to access application (north-south), but when the device is compromised by malware and the network communication behavior changes, the device starts to communicate with the finance server.

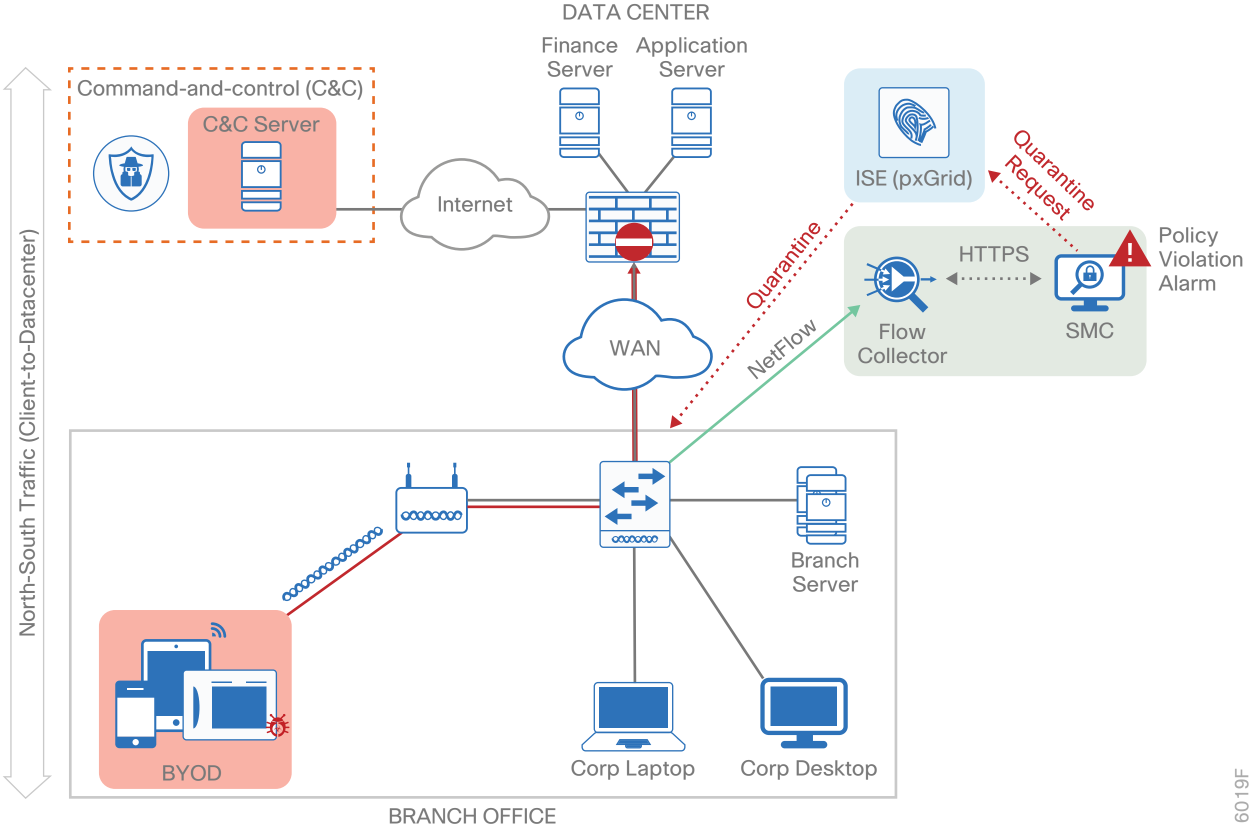
Figure 4 *Branch Office Network without NaaS Solution*



SOLUTION

When an employee uses his mobile device to start communicating with any Finance Server instead of application server, it's considered as an abnormal behavior in this scenario, whether the attempt is successful or not. Enabling NetFlow on the switches or WLCs gives deeper visibility into the network traffic behavior with Stealthwatch, and it can flag the unusual activity and alert as an anomalous behavior in SMC dashboard. This allows the admin to further investigate and quarantine a compromised device with a single click.

Figure 5 *Branch Office Network with NaaS Solution*

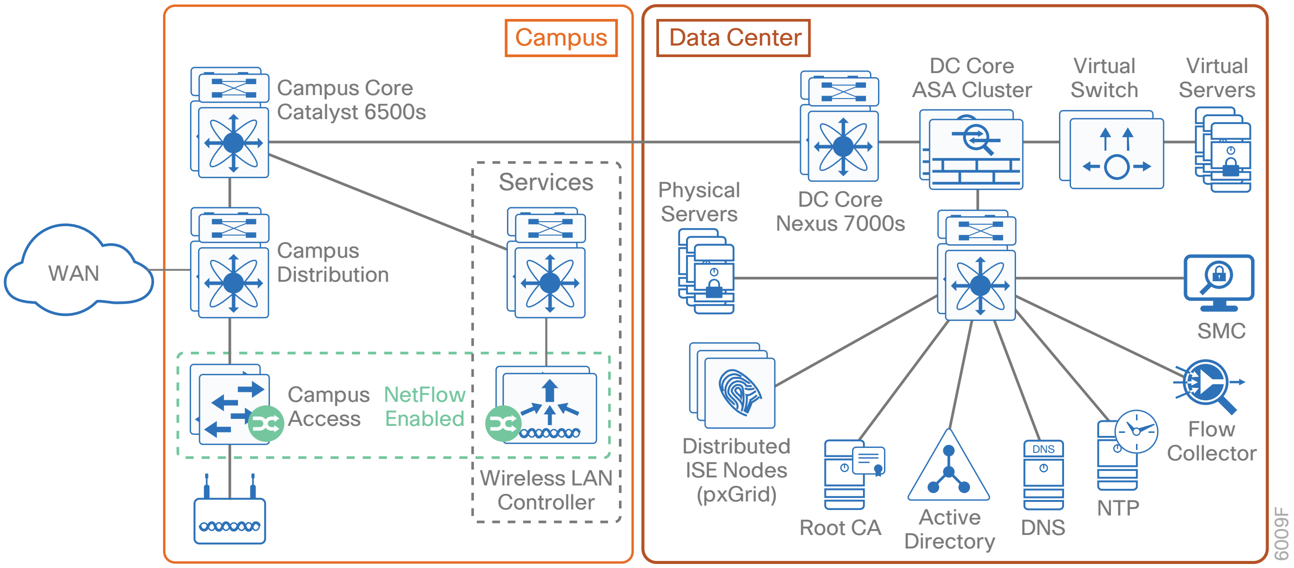


Design Overview

The NaaS solution provides comprehensive visibility into all network traffic through the use of Cisco NetFlow technology. Cisco NetFlow technology is supported across Cisco enterprise wireless LAN controllers, switches, and routers in order to enable complete non-performance-impacting telemetry to be implemented at all layers of the network. Coupling this enhanced visibility with identity and context information from the Cisco Stealthwatch, ISE and TrustSec solution enables security operators to better understand a network's traffic.

This guide focuses only on enabling NetFlow on Catalyst 3850 Switch and 5520/8540 Wireless LAN Controllers campus network access devices.

Figure 6 *Example network*



Tech Tip

CA Server is recommended for pxGrid certificates. NTP is required because time sync is needed for this solution to work.

Visibility into network traffic is provided through NetFlow export from Cisco WLC and switches, while identity services, including the user name and profile information, is provided through ISE. Stealthwatch Flow Collector provides NetFlow collection services and performs analysis in order to detect suspicious activity. Stealthwatch Management Console (SMC) provides centralized management for all Stealthwatch appliances and provides real-time data correlation, visualization, and consolidated reporting of combined NetFlow and identity analysis.

Deployment Details

The deployment described is based on several design and deployment guides that comprise the reference network architecture:

- Cisco Cyber Threat Defense v2.0 Design Guide
- Configuring pxGrid in an ISE Distributed Environment Guide
- Deploying Cisco Stealthwatch 6.7.1 with Cisco pxGrid Guide
- User-to-Data-Center Access Control Using TrustSec Deployment Guide
- Campus LAN and Wireless LAN Design Summary

IP addresses used in this guide are examples; you should use addressing that is applicable to your architecture.

Cisco ISE has different personas, or nodes, for which it can be configured:

- **Policy Administration Node (PAN)**—A node that runs the Administration persona
- **Monitoring and Troubleshooting Node (MnT)**—A node that runs the Monitoring persona
- **Policy Service Node (PSN)**—A node that runs the Policy Service persona
- **pxGrid**—A node that enables ecosystem partners to obtain user and device contextual information from ISE

For a standalone configuration in which the appliance uses all personas, the maximum number of end-points that can be supported is 10,000—dependent upon the installation hardware. To support a greater number of endpoints, to add additional resiliency, or to distribute policy services, you divide the personas across multiple physical or virtual appliances. In this example, there are five virtual nodes.

Two nodes are running both administration and monitoring personas: one is primary for these personas and one is secondary. Two additional nodes are running the Policy Service persona. One node is for the pxGrid service.

Tech Tip

Stealthwatch does not support pxGrid high availability.

This configuration offers resiliency and allows the deployment to scale to 10,000 endpoints for some hardware choices. To scale beyond 10,000 endpoints, you must deploy all personas on dedicated appliances. For more information about deployment size and scaling recommendations, see Cisco Identify Services Engine Hardware Installation Guide, Release 2.0.

Figure 7 Example pxGrid deployment

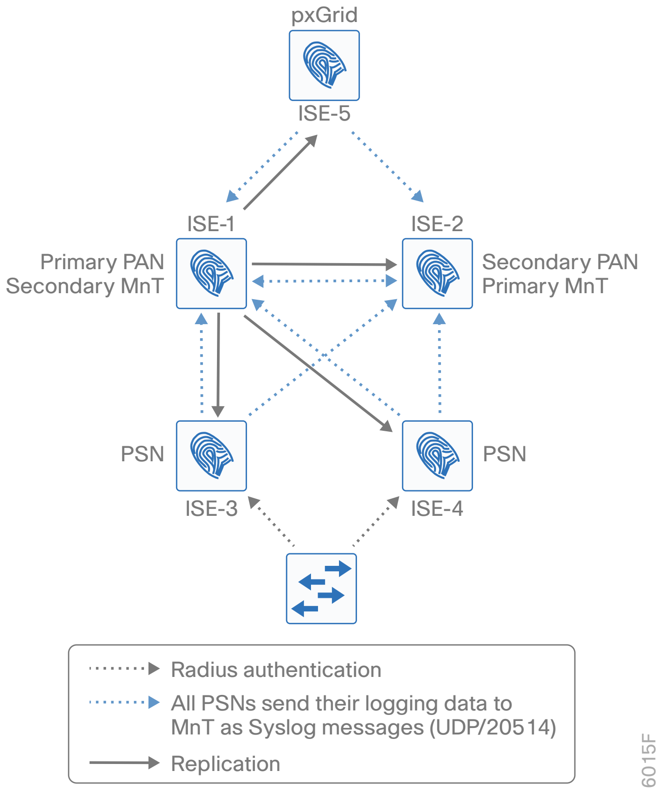


Table 1 Cisco ISE node IP addresses and hostnames

Device Persona	Shorthand	IP address	Hostname
Cisco ISE primary Policy Administration Node and secondary Monitoring and Troubleshooting node	Primary PAN Secondary MnT	10.4.48.41	ise-1.cisco.local
Cisco ISE secondary Policy Administration Node and secondary Monitoring and Troubleshooting node	Secondary PAN Primary MnT	10.4.48.42	ise-2.cisco.local
Cisco ISE Policy Service Node	First PSN	10.4.48.43	ise-3.cisco.local
Cisco ISE additional Policy Service Node	Additional PSN	10.4.48.44	ise-4.cisco.local
Cisco ISE pxGrid Node	pxGrid	10.4.48.45	pxgrid.cisco.local

Similarly to ISE, Stealthwatch also consists of different components: UDP Director (Replicator), Flow Sensor, Flow Collector, and SMC. Each has to be installed and configured separately. UDP Director and Flow Sensor are optional and are not covered in this guide.

The Flow Collector serves as a central collection point per location and analysis point for NetFlow data generated by all NetFlow generators. The Stealthwatch Management Console (SMC) acts as the single pane of glass to visualize this data, and this will be what a system admin will be interacting with most of the time.

Table 2 Stealthwatch node IP addresses and hostnames

Device Persona	Shorthand	IP address	Hostname
Stealthwatch Flow Collector	FC	10.4.48.70	fc1.cisco.local
Stealthwatch Management Console	SMC	10.4.48.71	smc1.cisco.local

PROCESS

Deploying Cisco ISE (pxGrid)

1. Install Cisco ISE (pxGrid) node
2. Create custom pxGrid certificate template (CA-signed)
3. Bind CA-signed pxGrid certificate on pxGrid node
4. Configure certificate trust list
5. Register and enable ISE pxGrid node operation

In this deployment, the Cisco ISE nodes are running as virtual machines. The installation process is detailed in the Campus 802.1X Authentication Technology Design Guide, and you should use it as a reference for complete step-by-step instructions on how to deploy fully distributed (Four Nodes) ISE environment.

This solution assumes that an ISE 2.0 Distributed Environment with the latest patches (see Appendix A) is already deployed and focuses on pxGrid Node only.

For more information, see the Cisco pxGrid design guides.

Procedure 1 Install Cisco ISE (pxGrid) node

Step 1: Boot new Cisco ISE.

Step 2: At the initial prompt, enter **setup**. The installation begins.

Step 3: Enter the host name, IP address, subnet mask, and default gateway of Cisco ISE.

```
Enter hostname[ ]: pxgrid
Enter IP address[ ]: 10.4.48.45
Enter IP netmask[ ]: 255.255.255.0
Enter IP default gateway[ ]: 10.4.48.1
```

Step 4: Enter Domain Name System (DNS) information.

```
Enter default DNS domain[ ]: cisco.local
Enter primary nameserver[ ]: 10.4.48.10
Add secondary nameserver? Y/N : N
```

Step 5: Configure the time.

```
Enter NTP server[time.nist.gov]: ntp.cisco.local
Add another NTP server? Y/N [N]: N
Enter system timezone[UTC]: PST8PDT
```

Step 6: Configure an administrator account.

You must configure an administrator account in order to access the CLI console. This account is not the same as the one used to access the GUI.

```
Enable SSH Service? Y/N [N]: Y
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]
```

Cisco ISE completes the installation and reboots. This process takes from several minutes to over an hour, depending on available resources. Do not press CTRL+C during the installation, or the installation aborts.

The installation procedure is now complete for Primary pxGrid ISE node. You need a Plus License for the pxGrid feature. For more information, see the Cisco ISE Ordering Guide.

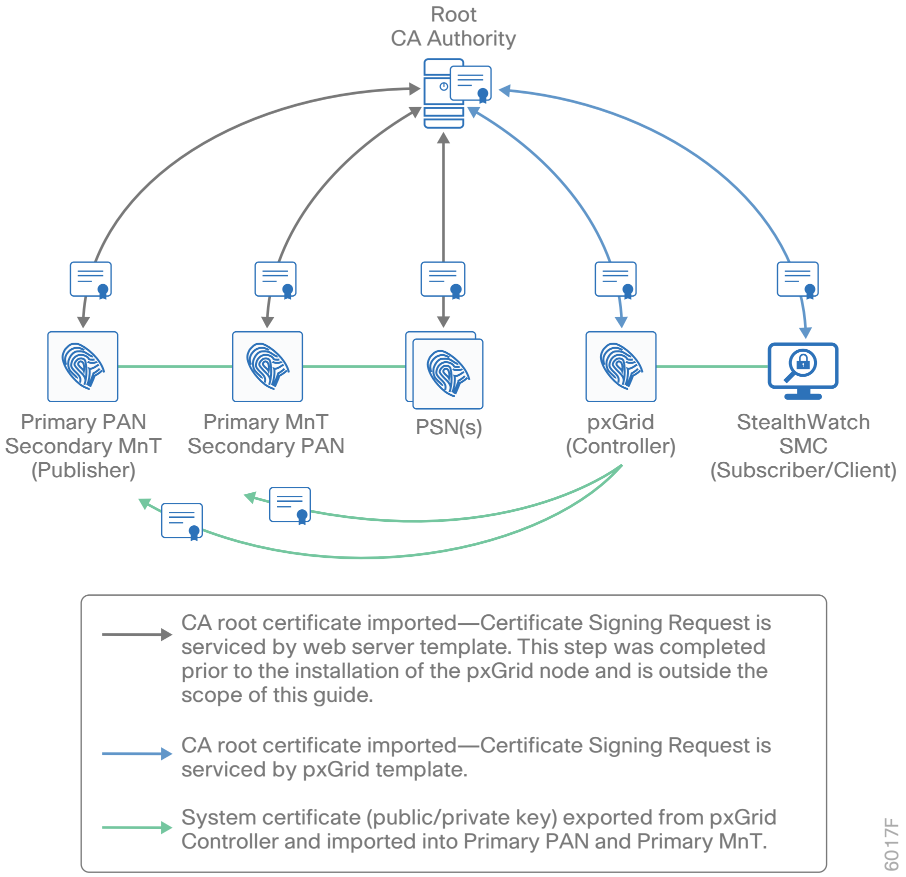
Tech Tip

After you have finished software installation, you should check the release notes to see if there are patches available to apply that are appropriate for the requirements of your organization. After you download any required patches, you can automatically distribute and apply them to all nodes by navigating to **Administration > System > Maintenance**, selecting Patch Management, and following the instructions. Minimum ISE 2.0 with Patch 2 is recommended for pxGrid and Stealthwatch 6.7.1 Integration. ISE Patch 2 upgrade will also enable **EPS Unquarantine button** under **Operations > Adaptive Network Control > Endpoint Assignment**.

For more information about Cisco ISE Design Considerations, refer to ISE configuration guides. For pxGrid, you may also refer to pxGrid design guides. For TrustSec design and deployment, see http://www.cisco.com/go/trustsec.

Procedure 2 Create custom pxGrid certificate template (CA-signed)

The pxGrid Custom-Template is required for pxGrid operation between the pxGrid Publisher (Cisco ISE) and pxGrid Subscriber/Client (Stealthwatch SMC) in a Certificate Authority (CA)-signed environment.



→ CA root certificate imported—Certificate Signing Request is serviced by web server template. This step was completed prior to the installation of the pxGrid node and is outside the scope of this guide.

→ CA root certificate imported—Certificate Signing Request is serviced by pxGrid template.

→ System certificate (public/private key) exported from pxGrid Controller and imported into Primary PAN and Primary MnT.

This solution assumes that an Enterprise CA Server was used as the CA Authority. The CA root certificate was imported into the trusted system certificates store of each of the ISE nodes. The Certificate Signing Request (CSR) node requests were serviced by the CA using the web server template and admin "usage" certificates defined in the ISE nodes, except for the pxGrid nodes, which will use the pxGrid Custom-Template created in this step.

Step 1: Login to Microsoft CA Server (example: MS Windows Server 2012).

Step 2: Navigate to **Control Panel > System and Security > Administrative Tools > Certification Authority**, and expand the Root CA Server (example: Root-CA).

Step 3: Right-click **Certificate Templates**, and then choose **Manage**. The Certificate Templates Console opens.

Step 4: In the Certificate Templates Console, right-click **User** Template, and then choose **Duplicate Template**.

Step 5: Click the **General** tab, and then rename the template **pxGrid**.

Step 6: Clear the **Publish certificate in Active Directory** checkbox.

Step 7: (Optional) Change the validity and renewal periods as required.

Step 8: Navigate to **Extensions tab > Application Policies** and click **Edit**.

Step 9: Click **Add**.

Step 10: Select **Server Authentication** and click **OK**.

Step 11: Remove **Encryption File System** and **Secure Email**. Click **OK**.

Step 12: Select **Issuance Policies**, and click **Edit**.

Step 13: Click **Add** and select **All issuance policies**. Click **OK**.

Step 14: Click **OK** to return to the template properties window.

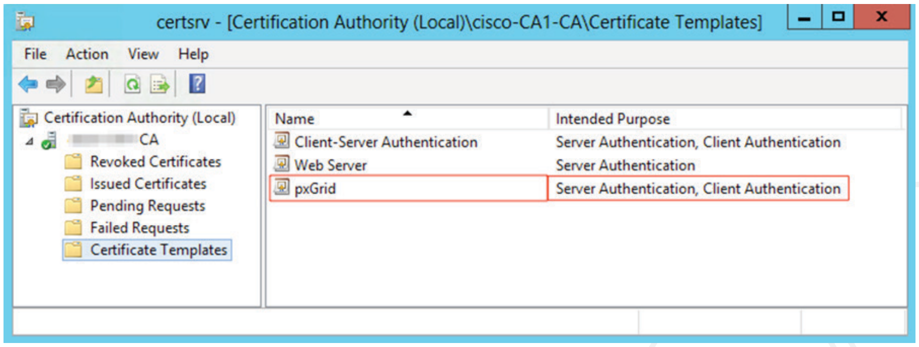
Step 15: On the **Subject Name** tab, choose **Supply in the request**.

Step 16: Click **Apply,** and then click **OK**.

Step 17: In the Certification Authority window, right-click **Certificate Template**, and then select **New > Certificate Template to issue**.

Step 18: Select the newly created pxGrid certificate template, and click **OK**.

Step 19: Verify that the custom pxGrid certificate template (with the intended purpose "Server Authentication, Client Authentication") is listed, along with Web Server and Client-Server Authentication certificates, as shown below:



certsrv - [Certification Authority (Local)\cisco-CA1-CA\Certificate Templates]

- Certification Authority (Local)
  - [redacted] CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

Name	Intended Purpose
Client-Server Authentication	Server Authentication, Client Authentication
Web Server	Server Authentication
pxGrid	Server Authentication, Client Authentication

For more detailed instructions, see Deploying Stealthwatch with Cisco pxGrid, which also includes instructions on Self-Signed Certificates.

Procedure 3 Bind CA-signed pxGrid certificate on pxGrid node

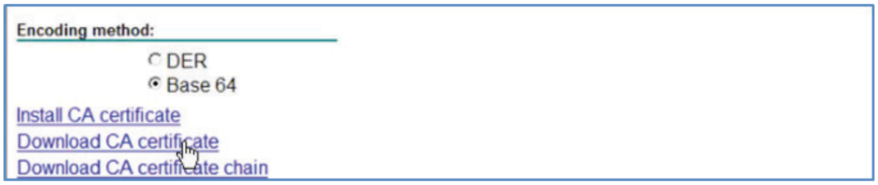
Step 1: In your browser, open the CA Server at https://ca.cisco.local/certsrv

Step 2: Select **Download a CA certificate, certificate chain, or CRL**.

Tech Tip

Even for hierarchical CA deployment, download the CA certificate and not the CA Certificate chain.

Step 3: Select **Base 64**, click **Download CA certificate**, and then save it (certnew.cer) to your local machine.



Encoding method:

○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain

Tech Tip

This solution uses ISE version 2.0; configuration steps and navigation paths in ISE version 1.4 and earlier may vary.

Step 4: In your browser, connect and login to the ISE pxGrid node in standalone mode (example: https://pxgrid.cisco.local).

Step 5: Navigate to **Administration > System > Certificates**, and in the left navigation pane, expand **Certificate Management** and select **Trusted Certificates**.

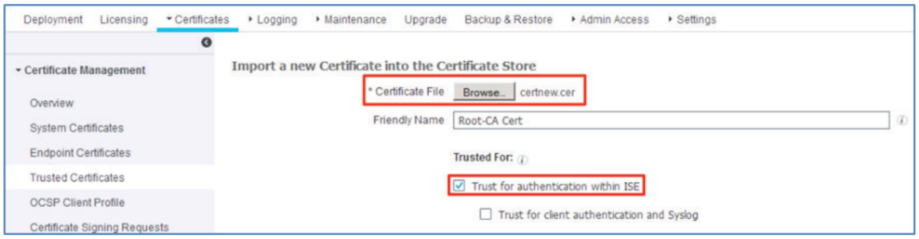
Step 6: Click **Import.**

Step 7: Click **Browse**.

Step 8: Enter the above-downloaded certificate.

Step 9: Select **Trust for authentication within ISE**.

Step 10: Click **Submit.** The certificate is imported into the Trusted Certificates store.



Import a new Certificate into the Certificate Store

* Certificate File: certnew.cer

Friendly Name: Root-CA Cert

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

Step 11: Navigate to **Administration > System > Certificates**, and in the left navigation pane, expand **Certificate Management** and select **Certificate Signing Requests.**

Step 12: Click **Generate Certificate Signing Requests (CSR)**.

Step 13: In the **Certificate(s) will be used for** list, choose **pxGrid**.

Step 14: Check the pxGrid node under **Node(s)**.

Step 15: Click **Generate.**

Step 16: Click **Export** and save the file on your local machine (example: pxGrid.pem).

Step 17: In your browser, open your CA Server (example: https://ca.cisco.local/certsrv).

Step 18: Select **Request a certificate**.

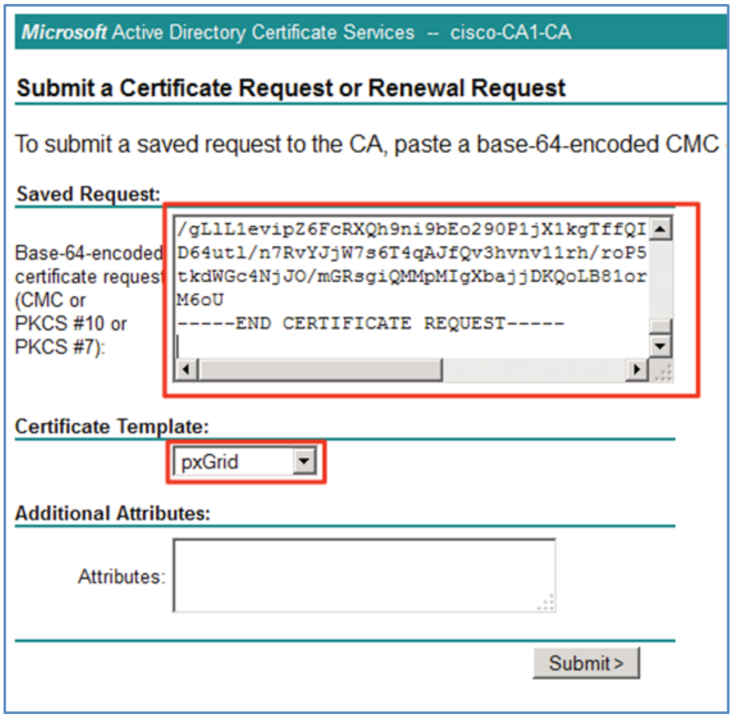
Step 19: Click **Submit a certificate request by using a base-64-encoded**.

Tech Tip

If you see the error "No Certificate Templates Could Be Found," see this Microsoft knowledge base article.

Step 20: Open the pxGrid.pem that was saved on your local machine earlier.

Step 21: Copy all content from pxGrid.pem and paste it in **Saved Request** box.



Microsoft Active Directory Certificate Services -- cisco-CA1-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
/gLlL1evipZ6FcRXQh9ni9bEo290P1jX1kgTffQI
D64utl/n7RvYJjW7s6T4qAJfQv3hvnv11rh/roP5
tkdWGc4NjJO/mGRsgiQMMpMIgXbajjDKQoLB81or
M6oU
-----END CERTIFICATE REQUEST-----
```

Certificate Template: pxGrid

Additional Attributes:

Attributes:

Step 22: In the **Certificate Template** list, choose **pxGrid**, and then click **Submit**.

Step 23: Select **Base-64** encoded format.

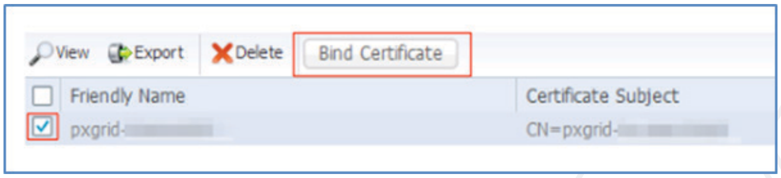
Step 24: Click **Download certificate** and save it to your local machine.

Step 25: Rename **certnew.cer** to **pxGrid-cert-signed-by-ca.cer.** This avoids any confusion with other generated certificates.

Step 26: In your browser, open the ISE pxGrid node (example: https://pxgrid.cisco.local).

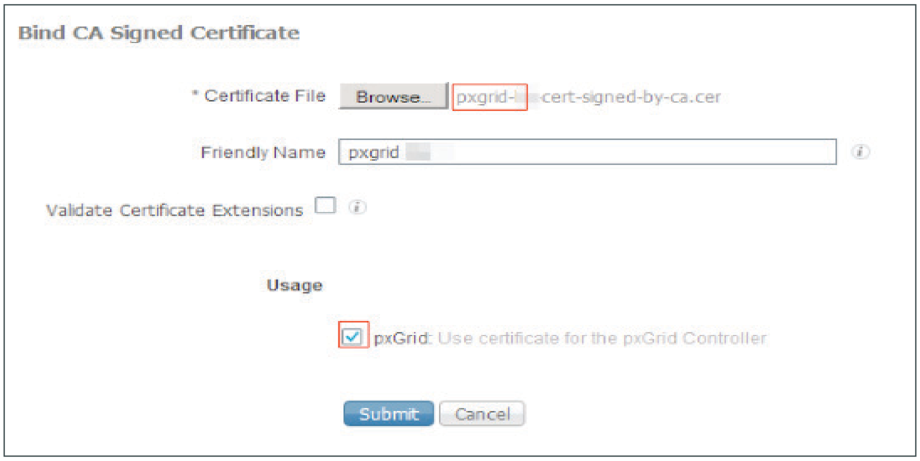
Step 27: Navigate to **Administration > System > Certificates**, and in the left navigation pane, expand **Certificate Management** and select **Certificate Signing Requests**.

Step 28: From the CSR(s) listed on the right, select the pxGrid CSR, and then click **Bind Certificate**.



☐	Friendly Name	Certificate Subject
☑	pxgrid-[redacted]	CN=pxgrid-[redacted]

Step 29: Browse to the **pxGrid-cert-signed-by-ca.cer** file downloaded earlier.



Bind CA Signed Certificate

* Certificate File pxgrid-[redacted]cert-signed-by-ca.cer

Friendly Name pxgrid [redacted]

Validate Certificate Extensions ☐

Usage

☑ pxGrid: Use certificate for the pxGrid Controller

Step 30: Under Usage, verify that **pxGrid** is selected, and then click **Submit**.

Step 31: In the dialog box requesting a restart, click **YES**. pxGrid node restarts.

Procedure 4 Configure certificate trust list

The nodes use public key infrastructure (PKI) to secure communications between them. So once the binding is completed in the previous step and pxGrid node restarts successfully, you can export the system certificate from pxGrid node and import it into Primary PAN and Primary MnT. In this deployment, you need to import the custom pxGrid template into both ISE-1 (Primary PAN) and ISE-2 (Primary MnT). If PAN and MnT are completely separate nodes you should separately import the certificates to individual PAN and MnT personas.

Step 1: In your browser, log in to the pxGrid node (example: https://pxgrid.cisco.local).

Step 2: If you receive certificate warnings, acknowledge them and continue.

Step 3: Navigate to **Administration > System > Certificates**, and in the left navigation pane, expand **Certificate Management** and choose **System Certificates**.

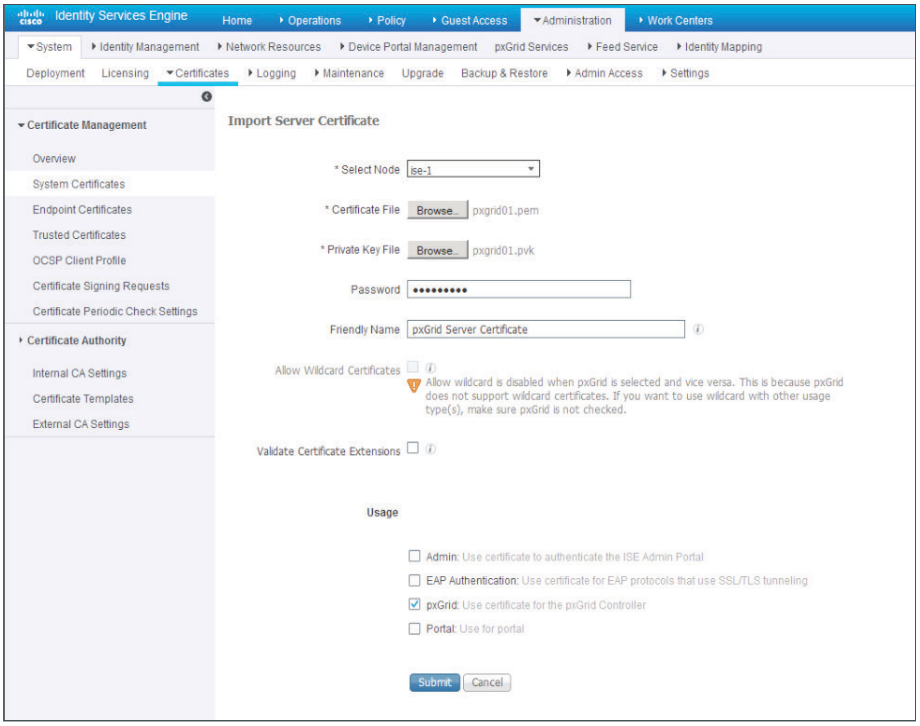
Step 4: Select **pxGrid certificate**, and then click **Export**.

Step 5: Select **Export Certificate and Private Key**, enter the private key (example: SecretKey), and then click **Export.** The file saves to the local machine.

Step 6: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 7: Navigate to **Administration > System > Certificates**, and in the left navigation pane, expand **Certificate Management**, choose **System Certificates**, and then click **Import**.

Step 8: In the **Select Node** list, ensure that **ise-1** (Primary PAN) is selected.



Import Server Certificate

* Select Node: ise-1

* Certificate File: pxgrid01.pem

* Private Key File: pxgrid01.pvk

Password: •••••••••

Friendly Name: pxGrid Server Certificate

Allow Wildcard Certificates ☐

Allow wildcard is disabled when pxGrid is selected and vice versa. This is because pxGrid does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrid is not checked.

Validate Certificate Extensions ☐

Usage

☐ Admin: Use certificate to authenticate the ISE Admin Portal
☐ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
☑ pxGrid: Use certificate for the pxGrid Controller
☐ Portal: Use for portal

Step 9: Next to Certificate File, click **Browse**.

Step 10: Enter the Certificate (.pem) and Private Key (.pvk) files exported from the pxGrid node earlier, and then click **Submit**.

Step 11: In the **Select Node** list, choose **ise-2** (Primary MnT).

Step 12: Next to Certificate File, click **Browse**.

Step 13: Enter the Certificate (.pem) and Private Key (.pvk) files exported from the pxGrid node earlier, and then click **Submit**.

Procedure 5 Register and enable ISE pxGrid node operation

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to **Administration > System > Deployment**, click **Register**, and then choose **Register an ISE Node**.

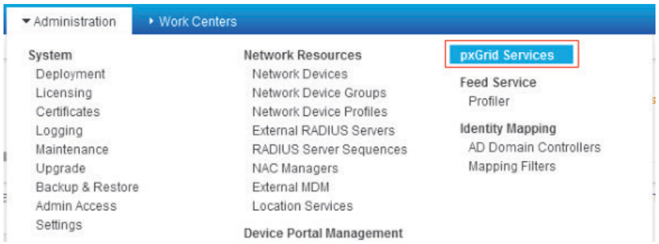
Step 3: Enter values for the FQDN, user name and password, and then click **Next**. The pxGrid registers and re-starts.

Step 4: Navigate to **Administration > System > Deployment**, select **pxGrid node**, and then click **Edit**.

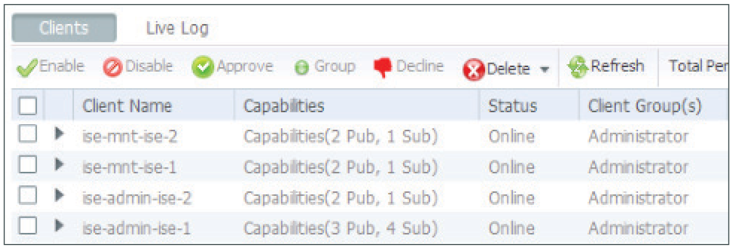
Step 5: In General Settings, clear all personas (Administrator, Monitoring and Policy Service), leaving only **pxGrid** selected.

Step 6: Click **Save**.

Step 7: Navigate to **Administrator > pxGrid Services**.

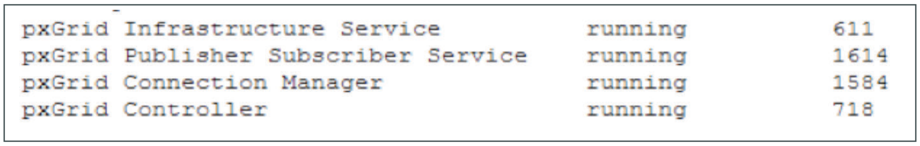


Step 8: In the Clients tab, verify that published client names (example: ise-admin-ise-1) appear.



☐		Client Name	Capabilities	Status	Client Group(s)
☐	▶	ise-mnt-ise-2	Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	▶	ise-mnt-ise-1	Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	▶	ise-admin-ise-2	Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	▶	ise-admin-ise-1	Capabilities(3 Pub, 4 Sub)	Online	Administrator

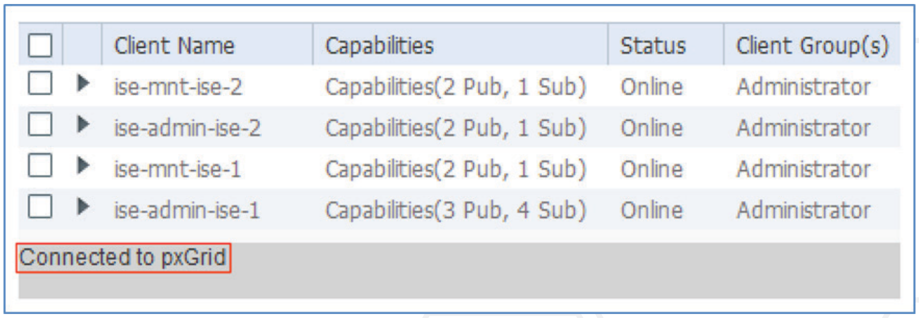
In the ISE (pxGrid) console, verify that the pxGrid services are running by entering **show application status ise** command. This may take a while to appear.



```
pxGrid Infrastructure Service          running          611
pxGrid Publisher Subscriber Service    running          1614
pxGrid Connection Manager              running          1584
pxGrid Controller                      running          718
```

Step 9: If Auto-Registration is disabled, click **Enable Auto-Registration**.

Step 10: Verify that you are connected to pxGrid.



☐		Client Name	Capabilities	Status	Client Group(s)
☐	▶	ise-mnt-ise-2	Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	▶	ise-admin-ise-2	Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	▶	ise-mnt-ise-1	Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	▶	ise-admin-ise-1	Capabilities(3 Pub, 4 Sub)	Online	Administrator

Connected to pxGrid

PROCESS

Deploying Cisco Stealthwatch

1. Install Cisco Stealthwatch
2. Upload CA root certificate into Stealthwatch trusted store
3. Enable SSH on SMC via web client
4. Generate CSR request on SMC
5. Sign the pxGrid Client CSR request
6. Upload SMC identity certificate to SSL client identities

Procedure 1 Install Cisco Stealthwatch

This document assumes that Stealthwatch 6.7.1 is already installed and licensed. If not, install and configure Stealthwatch Virtual-Appliances in the following order:

1. **Flow Collector VE (Mandatory)**
2. **SMC VE (Mandatory)**

For step-by-step installation instructions, refer to the **SMC VE and Flow Collector VE Installation and Configuration Guide** from the Stealthwatch download center.

UDP Director and Flow Sensor are optional and are not part of the initial NaaS Solution Validation.

Tech Tip

Make sure to configure the Network Time Protocol (NTP) and system time (the UTC time zone is highly recommended) settings on both Stealthwatch SMC and Flow Collector before proceeding.

Procedure 2 Upload CA root certificate into Stealthwatch trusted store

Step 1: In your browser, log in to the CA-Server (example: https://ca.cisco.local/certsrv).

Step 2: Click **Download a CA certificate, certificate chain, or CRL**.

Step 3: Select **Base 64**, and then click **Download CA certificate**.

Step 4: Save the Root-CA certificate (root-ca.crt) on your local machine.

Step 5: In your browser, log in to the SMC (example: https://smc1.cisco.local).

Step 6: Navigate to **Admin User > Administer Appliance**.

Step 7: From the side navigation, select **Configuration > Certificate Authority Certificates**.

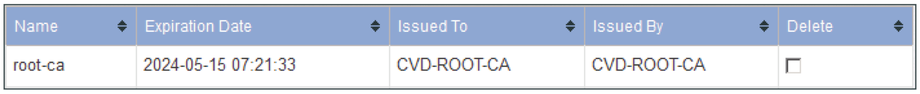
Step 8: Click **Browse** and upload the **root-ca.crt** file.

Step 9: Enter Name, and then click **Add Certificate**.

Tech Tip

For **Name**, use underscores/hyphen and do not use spaces.

Step 10: Under Certificate Authority Certificates, verify that **root-ca** certificate is listed.



Name	Expiration Date	Issued To	Issued By	Delete
root-ca	2024-05-15 07:21:33	CVD-ROOT-CA	CVD-ROOT-CA	☐

Tech Tip

If you have a Two Tier (Root & Subordinate) PKI CA (Certificate Authority) Hierarchy Deployment you may also upload the subordinate CA certificate (example: sub-ca.crt).

Procedure 3 Enable SSH on SMC via web client

Step 1: In your browser, log in to the SMC (example: https://smc1.cisco.local).

Step 2: Navigate to **Admin User > Administer Appliance**.

Step 3: From the side navigation, select **Configuration > Services**.

Step 4: Select **Enable SSH,** and then select **Enable Root SSH Access**.

Step 5: Click **Apply**.

Procedure 4 Generate CSR request on SMC

In this procedure, you generate the SMC private key, the certificate-signing request (CSR) to be signed by the CA authority. The CA template for pxGrid must contain an EKU of both client authentication and server authentication to be valid for pxGrid operation.

Step 1: Log in to SMC via the SSH client (example: Putty) and generate a private key.

```
openssl genrsa -out smc.key 4096
```

Step 2: Generate a SMC CSR request to be signed by the CA server.

```
openssl req -new -key smc.key -out smc.csr
```

Step 3: Copy the smc.csr and smc.key to your local machine from the SMC client. The certificate and key are used in the next procedure.

Tech Tip

Use an FTP Client (example: FileZilla) and connect to SMC client to download the certificate (smc.crt) and key (smc.key).

Procedure 5 Sign the pxGrid Client CSR request

Step 1: In your browser, open your CA Server (example: https://ca.cisco.local/certsrv).

Step 2: Click **Request a certificate**.

Step 3: Click **Submit a certificate request by using a base-64-encoded**.

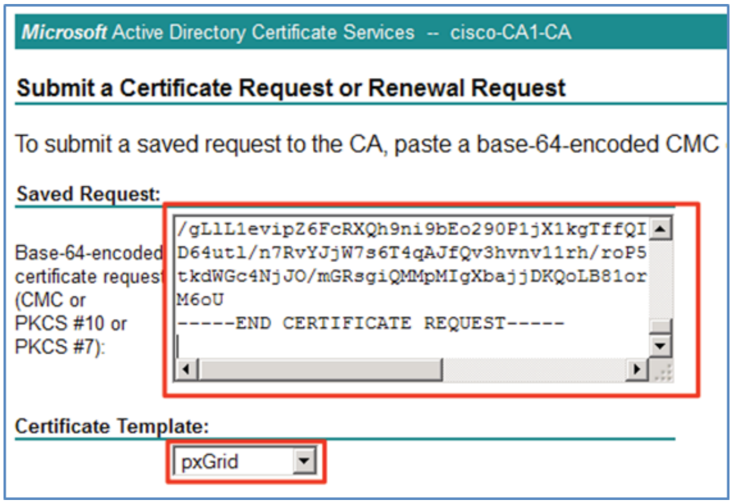
Step 4: In a text-editor, open smc.csr, which you downloaded from the SMC client in the previous procedure, and copy all content.

Tech Tip

Example of the content inside the smc.csr file:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErzCCApcCAQAwajELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNBTElGT1JOSUEx
DDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ0lTQ08xDTALBgNVBAsMBENTU0cxGTAX
BgNVBAMMEHNtYzEuY2lzY28ubG9jYWwwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAw
-----END CERTIFICATE REQUEST-----
```

Step 5: In **Saved Request**, paste the content that you copied from smc.csr.



Microsoft Active Directory Certificate Services -- cisco-CA1-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
/gLlL1evipZ6FcRXQh9ni9bEo290P1jX1kgTffQI
D64utl/n7RvYJjW7s6T4qAJfQv3hvnv11rh/roP5
tkdWGc4NjJO/mGRsgiQMMpMIgXbajjDKQoLB81or
M6oU
-----END CERTIFICATE REQUEST-----
```

Certificate Template: pxGrid

Step 6: In the **Certificate Template** list, choose **pxGrid**, and then click **Submit**.

Step 7: Download the certificate in a base-64 encoded format (example: certnew.cer).

Step 8: Rename **certnew.cer** to **smc-ca-signed.cer**

Step 9: Change the extension of the certificate file from **smc-ca-signed.cer** to **smc-ca-signed.crt**. In next two procedures, only the **.crt** extension is accepted.

Tech Tip

Procedure 5 is a new step in Stealthwatch v6.7.1, and the certificate with the .crt extension is required for it. This certificate is used for pxGrid client authentication. If you are having troubling uploading the SSL client certificate, try using Google Chrome.

Tech Tip

For the initial connection between SMC and ISE (when setting up the attribution configuration), it is necessary that SMC trusts the ISE certificate. But ISE does not need to trust the SMC Identity Certificate. Hence uploading the SMC identity certificate to SSL Server Identity is not recommended.

Procedure 6 Upload SMC identity certificate to SSL client identities

Step 1: In your browser, log in to SMC (example: https://smc1.cisco.local).

Step 2: Navigate to **Admin User > Administer Appliance**.

Step 3: From the left sidebar, navigate to **Configuration > SSL Certificate.**

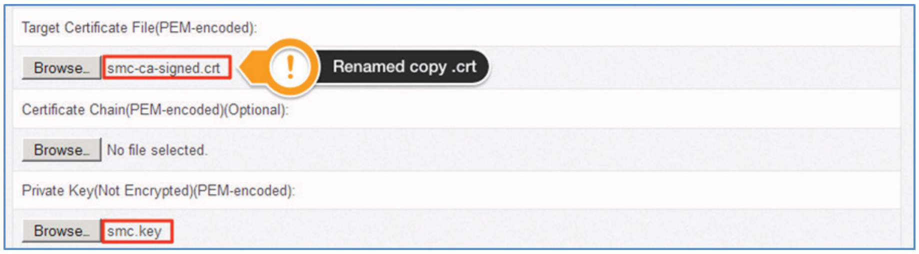
Step 4: Under **SSL Client Identity**, enter a friendly name (example: pxGrid-SSL-Client).

Tech Tip

For the friendly name, use underscores/hyphens instead of spaces.

The above Client SSL Certificate pxGrid-SSL-Client is selected later, when adding ISE nodes and enabling Cisco ISE Mitigation in SMC.

Step 5: Upload the SMC public certificate **smc-ca-signed.crt** file and private key pair.



Target Certificate File(PEM-encoded): smc-ca-signed.crt

Certificate Chain(PEM-encoded)(Optional): No file selected.

Private Key(Not Encrypted)(PEM-encoded): smc.key

Step 6: Click **Upload Certificate**, and then click **OK**.

Tech Tip

Use the same Certificate Authority (CA) Server to issue both ISE Identity and pxGrid certificates.

The restart may take 30 minutes or more. If the message “SMBus Host Controller not enabled” appears in the console, ignore it.

PROCESS

Integrating Cisco ISE with Cisco Stealthwatch

1. Configure receipt of syslog events from Cisco ISE
2. Add ISE MnT and PSN nodes
3. Verify pxGrid services and switch to Endpoint Protection Services
4. Enable Active Directory configuration in SMC
5. Launch SMC desktop Java client for Windows
6. Enabling Java store to trust the CA certificate

Now that you have successfully installed and licensed Cisco ISE (pxGrid Publisher) and Stealthwatch (pxGrid Client), you can proceed with the integration.

Procedure 1 Configure receipt of syslog events from Cisco ISE

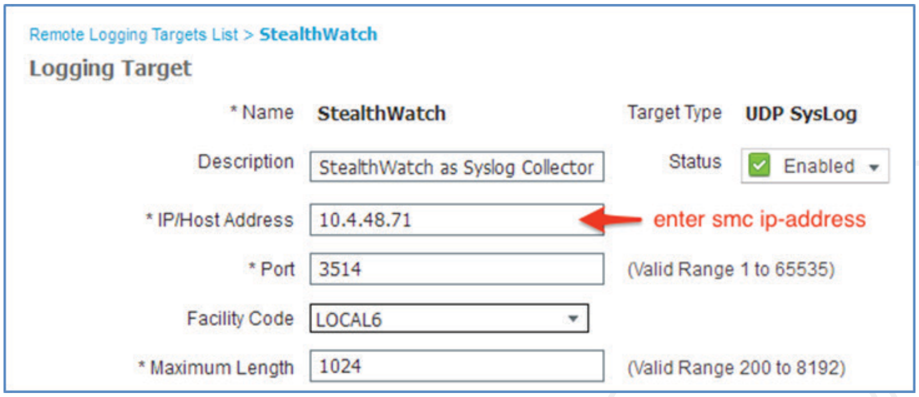
Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to **Administrator > System > Logging > Remote Logging Targets**.

Step 3: Click **Add**.

Step 4: For Logging Target, enter the details for the Stealthwatch SMC. (Do not enter the Flow Collector IP address, or else ISE Syslog details will not be received by Stealthwatch.)

- Name: **Stealthwatch**
- IP/Host Address: **smc-ip-address** (example: 10.4.48.71)
- Port: **3514** (Cisco's Recommended Port)



Remote Logging Targets List > **StealthWatch**

Logging Target

* Name	**StealthWatch**	Target Type	**UDP SysLog**
Description	StealthWatch as Syslog Collector	Status	☑ Enabled
* IP/Host Address	10.4.48.71	enter smc ip-address	
* Port	3514	(Valid Range 1 to 65535)	
Facility Code	LOCAL6		
* Maximum Length	1024	(Valid Range 200 to 8192)	

Tech Tip

SMC defaults to listening on port 3514. If you choose to configure ISE with a different destination port, you need to change the configuration of the SMC, as well. Do not use port 514 or port 8514, because those are reserved for other services on SMC.

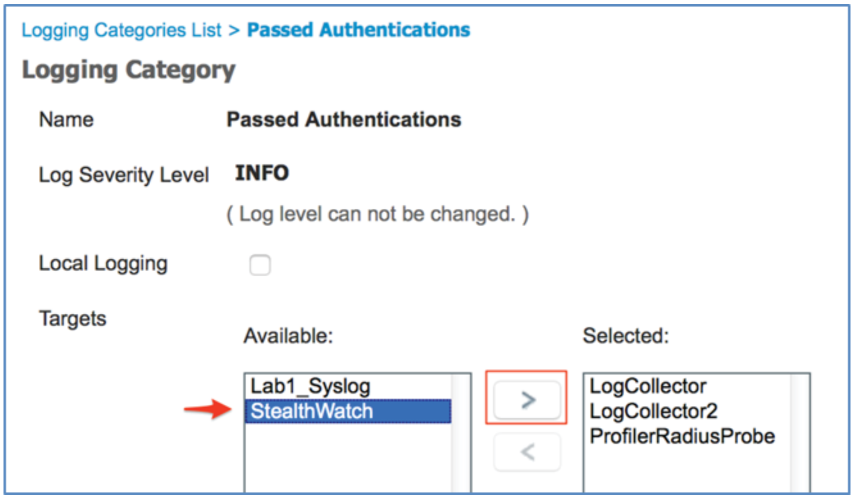
Step 5: Click **Submit**.

Step 6: From the left navigation pane, select **Logging Categories**.

Step 7: Enable syslog message for the following four categories Passed Authentications, Radius Accounting, Profiler, and Administrative and Operational Audit.

Step 8: In the **Logging Categories** list, choose **Passed Authentications**.

Step 9: Move the target named **Stealthwatch** from Available to Selected, as shown.



Name **Passed Authentications**

Log Severity Level **INFO**

(Log level can not be changed.)

Local Logging ☐

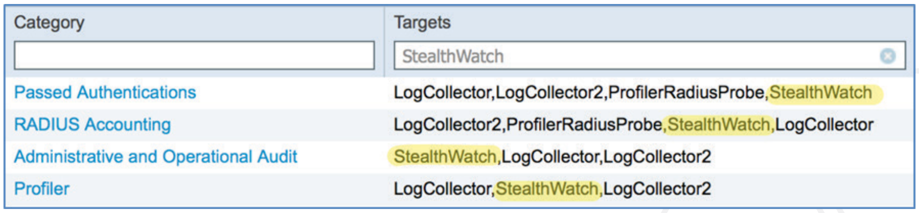
Targets

Available:
Lab1_Syslog
StealthWatch

Selected:
LogCollector
LogCollector2
ProfilerRadiusProbe

Step 10: Repeat the steps 8-9 for the three more logging categories: Radius Accounting, Profiler, and Administrative and Operational Audit.

Step 11: Filter the Targets column and make sure Stealthwatch has been added to all four categories, as shown.



Category	Targets
	StealthWatch
Passed Authentications	LogCollector,LogCollector2,ProfilerRadiusProbe,StealthWatch
RADIUS Accounting	LogCollector2,ProfilerRadiusProbe,StealthWatch,LogCollector
Administrative and Operational Audit	StealthWatch,LogCollector,LogCollector2
Profiler	LogCollector,StealthWatch,LogCollector2

Procedure 2 Add ISE MnT and PSN nodes

Now you configure the Cisco ISE MnT and PSN nodes so that you can receive syslog messages from the Cisco ISE device in order to provide identity data to Stealthwatch for hosts on your network.

Step 1: In your browser, log in to SMC (example: https://smc1.cisco.local).

Step 2: Navigate to **Tools > Settings > Cisco ISE Configuration**.

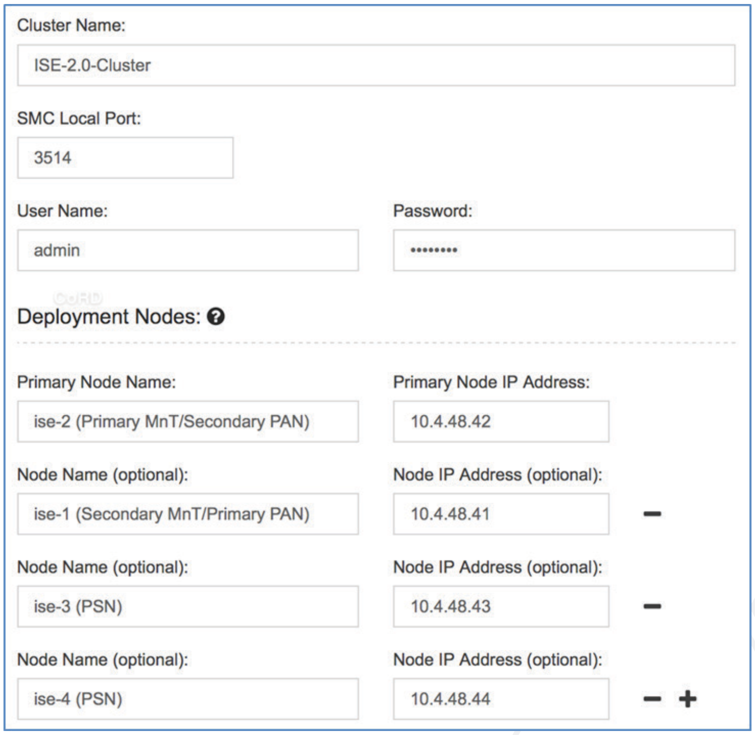
Step 3: Enter the **ISE Cluster Name**.

Step 4: Leave the SMC Local Port as **3514**.

Step 5: Enter the ISE login User Name and Password. You must enter a super-admin user (example: admin) in order to authenticate ISE.

Step 6: Under Deployment Nodes, add the following:

- Primary Node Name: **ise-2** (Primary MnT / Secondary PAN)
- Primary Node IP Address: **10.4.48.42**
- Node Name (optional): **ise-1** (Secondary MnT / Primary PAN)
- Node IP Address: **10.4.48.41**



Cluster Name: ISE-2.0-Cluster

SMC Local Port: 3514

User Name: admin

Password: ••••••••

Deployment Nodes:

Primary Node Name: ise-2 (Primary MnT/Secondary PAN)

Primary Node IP Address: 10.4.48.42

Node Name (optional): ise-1 (Secondary MnT/Primary PAN)

Node IP Address (optional): 10.4.48.41

Node Name (optional): ise-3 (PSN)

Node IP Address (optional): 10.4.48.43

Node Name (optional): ise-4 (PSN)

Node IP Address (optional): 10.4.48.44

Tech Tip

Because SMC primarily talks to MnT nodes in order to receive syslog data (and in this case, ise-2 is the Primary MnT), you must add ise-2 before ise-1. If the PAN Node is separate from MnT or PSN, you don't need to add PAN node, because they do not transmit the relevant syslog messages. To add more ISE nodes, click the + icon next to the **Node IP Address (optional)** input field.

Additionally, in order to see the authenticated users listed under **Network > Users** in the SMC Web Client, you must add all PSNs.

Step 7: Click **Save**, and then check the sync-up status indicator between ISE and SMC. If the communication is successful, the Add Cisco ISE Mitigation button is visible. If the Add Cisco ISE Mitigation button is missing, go back to the Procedure 1 in this process and ensure that all four logging categories in ISE Syslog are properly configured.

Step 8: Click **Add Cisco ISE Mitigation**.

Step 9: In the Certificate Selection list, choose the **pxGrid-SSL-Client** certificate that you created in Procedure 6, "Upload SMC Identity Certificate to SSL Client Identities."

Step 10: Under Migration Nodes, add Primary pxGrid Node.

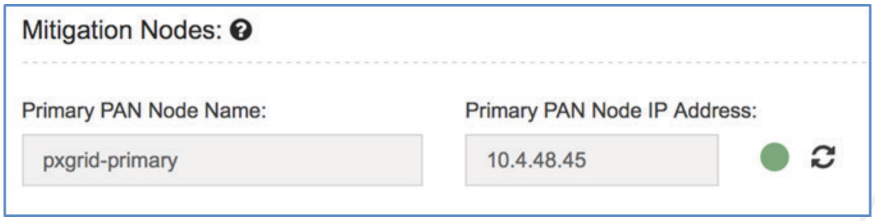
- Primary PAN Node Name: **pxgrid-primary**
- Primary Node IP Address: **10.4.48.45**

Tech Tip

If you run into any issues adding pxGrid node, try using Google Chrome.

Step 11: Click **Save**.

Step 12: Wait for the Success notification, and then click **OK**. The green sync-up indicator appears.



Mitigation Nodes:

Primary PAN Node Name: pxgrid-primary

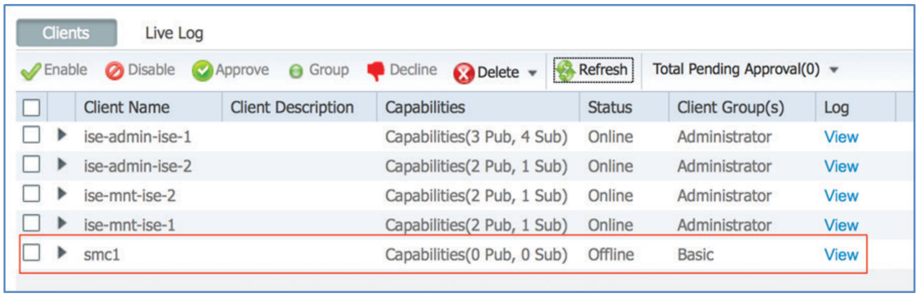
Primary PAN Node IP Address: 10.4.48.45

Procedure 3 Verify pxGrid services and switch to Endpoint Protection Services

Only after successfully adding pxGrid node in SMC (under Cisco ISE Mitigation) as shown above are you able to see smc listed in ISE under Clients (as shown in Step 2).

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

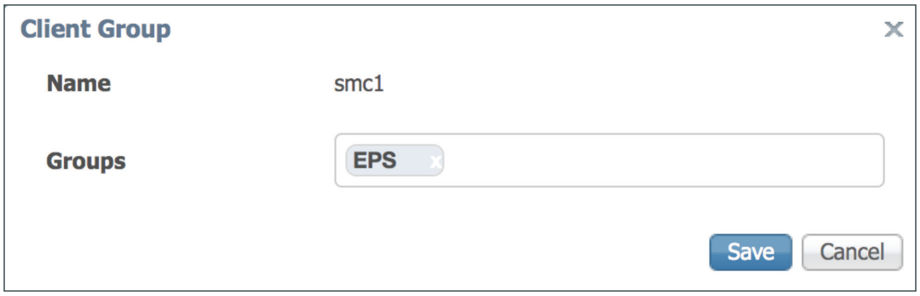
Step 2: Navigate to **Administration > pxGrid Services > Clients** and verify that smc1 is registered as a pxGrid client.



☐		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
☐	▶	ise-admin-ise-1		Capabilities(3 Pub, 4 Sub)	Online	Administrator	View
☐	▶	ise-admin-ise-2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
☐	▶	ise-mnt-ise-2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
☐	▶	ise-mnt-ise-1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
☐	▶	smc1		Capabilities(0 Pub, 0 Sub)	Offline	Basic	View

Step 3: Select **smc1**, and then click **Group**.

Step 4: Delete the default Groups setting **Basic** (click the **X**), and then in the **Groups** list, choose **EPS**.

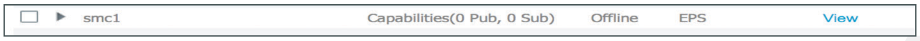


Name smc1

Groups EPS

Step 5: Click **Save**.

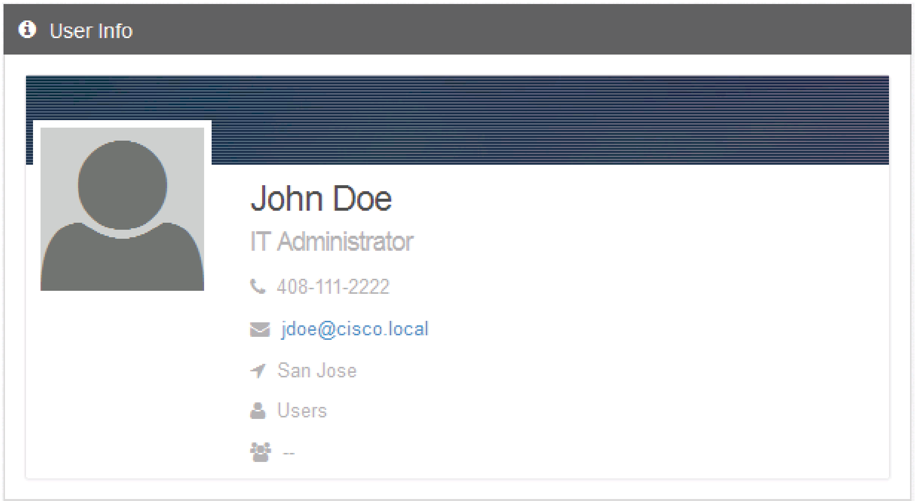
Step 6: Verify that the smc1 client group has changed to the EPS group.



☐	▶	smc1	Capabilities(0 Pub, 0 Sub)	Offline	EPS	View

Procedure 4 Enable Active Directory configuration in SMC

Stealthwatch offers more visibility when you configure Active-Directory in SMC. After SMC starts querying Active-Directory, the User Info section will be populated, as shown.



John Doe
IT Administrator
☎ 408-111-2222
jdoe@cisco.local
San Jose
Users
--

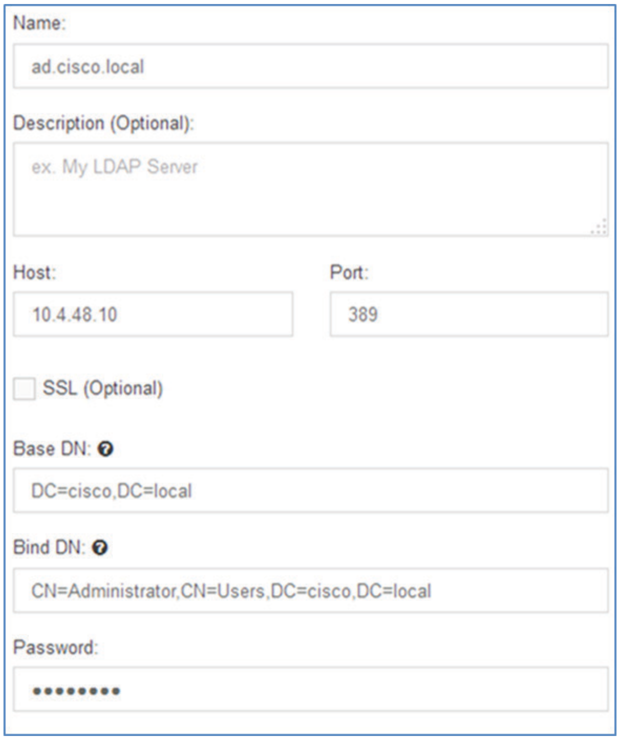
Step 1: In your browser, log in to SMC (example: https://smc1.cisco.local).

Step 2: Navigate to **Tools > Settings > Active Directory Configuration**.

Step 3: Click **Add new configuration**.

Step 4: Enter the **Active Directory Lookup Configuration** details, for example:

- Name: **ad.cisco.local**
- Host: **10.4.48.10**
- Port: **389**
- Base DN: **DC=cisco,DC=local**
- Bind DN: **CN=Administrator,CN=Users,DC=cisco,DC=local**
- Password: **C1sco123**



Name: ad.cisco.local

Description (Optional): ex. My LDAP Server

Host: 10.4.48.10

Port: 389

☐ SSL (Optional)

Base DN: DC=cisco,DC=local

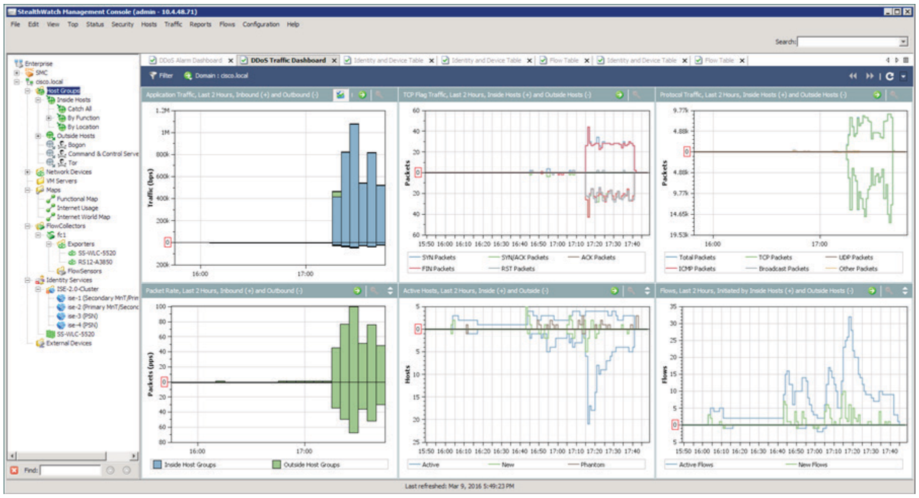
Bind DN: CN=Administrator,CN=Users,DC=cisco,DC=local

Password: ••••••••

Step 5: Click **Save**.

Procedure 5 Launch SMC desktop Java client for Windows

Until now you have only used the SMC Web Client. For additional control and visibility, you must enable the Java client.


StealthWatch Management Console (admin - 10.4.48.71)
File Edit View Top Status Security Hosts Traffic Reports Flows Configuration Help
Search:
DDoS Alarm Dashboard
DDoS Traffic Dashboard
Identity and Device Table
Flow Table
Filter
Domain : cisco.local
Enterprise
SMC
cisco.local
Host Groups
Application Traffic, Last 2 Hours, Inbound (+) and Outbound (-)
TCP Flag Traffic, Last 2 Hours, Inside Hosts (+) and Outside Hosts (-)
Protocol Traffic, Last 2 Hours, Inside Hosts (+) and Outside Hosts (-)
Packet Rate, Last 2 Hours, Inbound (+) and Outbound (-)
Active Hosts, Last 2 Hours, Inside (+) and Outside (-)
Flows, Last 2 Hours, Initiated by Inside Hosts (+) and Outside Hosts (-)
Inside Host Groups
Outside Host Groups
Find:
Last refreshed: Mar 9, 2016 5:49:23 PM

Step 1: In your browser, log in to the SMC Web GUI (example: https://smc1.cisco.local).

Step 2: Click **Launch SMC.**

If you receive an error while launching the SMC client, the issue is most likely related to the SSL certificate. Proceed to Procedure 5.

Procedure 6 Enabling Java store to trust the CA certificate

(Optional)

Follow this procedure only if you received an error message when launching the SMC client. Otherwise, skip to "Enabling NetFlow on Network Device."

Step 1: If you receive an error while launching the SMC client, the issue is most likely related to the SSL certificate. Proceed to step 4.

Step 2: On your Windows machine, which will run the SMC Java client, navigate to **C:\Program Files\Java\jre7\lib\security\** and locate the **cacerts** file.

Tech Tip

Based on the version of Java you might have to change the path accordingly.

Step 3: Right-click the **cacerts** file and choose **Properties**.

Step 4: On the Security tab, click **Edit**.

Step 5: Enter a user name.

Step 6: Next to Full Control, select **Allow**.

Step 7: Click **Apply**, and then click **OK** twice.

Step 8: Locate the path of root-ca certificate (example: C:\root-ca.crt) that you downloaded on your local machine in Procedure 2, “Upload CA root certificate into Stealthwatch Trusted Store.”

Step 9: At the Windows command prompt, change the directory.

```
cd C:\Program Files\Java\jre7\bin\
```

Step 10: Insert the root certificate into the key store.

```
keytool -keystore "C:\Program Files\Java\jre7\lib\security\cacerts" -importcert
-alias root-cert -file "C:\root-ca.crt"
```

Tech Tip

If the above command fails, verify that all of the paths in the command above are correct.

If keytool is not available, you may need to install the Java Development Kit. For more information, see [Configuring pxGrid in an ISE Distributed-Environment Guide.]

Step 11: Enter the password **changeit,** and then repeat the password.

Step 12: Opt to trust the certificate.

Step 13: Return to the SMC Web GUI (example: https://smc1.cisco.local) and click **Launch SMC**. The Java client starts.

Tech Tip

For debugging, you can enable the Java Console. Navigate to **Control Panel > Java > Advanced tab,** and under Java Console, select **Show Console** and click **Apply** and then **OK.**

ENABLING NETFLOW ON NETWORK DEVICES

This guide covers enabling NetFlow on only campus/branch network access devices, the Catalyst 3850 Switch and 5520/8540 Wireless LAN Controllers. For information about enabling NetFlow on other devices, see the NetFlow Configuration Stealthwatch Wiki page.

Table 3 *NetFlow Validated Performance Data*

Model	Aps	Clients	Throughputs	Max Flows
8540	3000	32000	17 Gbps	200000
5520	750	10000	7 Gbps	200000
3850	24	1000	2 Gbps	4000

This solution assumes that the C3850 switch and WLC 5520/8540 are configured and added as network devices (in Cisco ISE under Administration > Network Resources > Network Devices). For more information about adding network devices, see the Campus 802.1X Authentication Technology Design Guide.

There are three components for FnF configuration: Flow Record, Flow Exporter, and Flow Monitor. After you have configured all three components, you apply the Flow Monitor to a wired or wireless interface such as a L2/L3 port, VLAN, or WLAN (SSID). Lastly, you configure AVC for deeper visibility.

Flow Record

A *Flow Record* defines the information that will be gathered by the NetFlow process, such as packets in the flow and the types of counters gathered per flow. Custom flow records specify a series of *match* and *collect* commands that tell the Cisco device which fields to include in the outgoing NetFlow record.

The match fields are the key fields, meaning that they are used to determine the uniqueness of the flow.

The collect fields are extra information that is included in the record in order to provide more detail to the collector for reporting and analysis.

When you configure Flow Record, you are telling the device to show all of the flow data traffic that enters (Ingress) or leaves (Egress) the device.

Flow Exporter

The *Flow Exporter* defines where and how to send the NetFlow (Flow Records). In actuality a Flow Exporter defines a flow collector IP address and port as the destination, and in this case the Stealthwatch Flow Collector is the destination.

Flow Monitor

A *Flow Monitor* describes the NetFlow cache or information stored in the cache. Additionally, the Flow Monitor links together the Flow Record and the Flow Exporter.

The Flow Monitor includes various cache characteristics such as the timers for exporting, the size of the cache, and, if required, the packet sampling rate.

As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch Flow Collector.

A flow is ready for export when it is inactive for a certain time (for example, no new packets received for the flow); or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download). There are timers to determine if a flow is inactive or if a flow is long lived.

Application Visibility and Control

AVC classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine and provides application-level visibility and control into Wi-Fi networks. After the applications are recognized, the AVC feature enables you to either drop or mark the data traffic.

Using AVC, you can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link use, and infrastructure upgrades.

Tech Tip

On Catalyst 3850 switch code 3.6.4, AVC is not supported on wired and wireless as part of NaaS Solution.

Wired AVC (NBAR2) will be available in 16.3.1, but Flexible NetFlow (FNF) support on wired AVC (NBAR2) will be available in 16.3.2. Therefore exporting flow record **match application name** to external collector such as Stealthwatch is not available until 16.3.2.

AVC is supported and functional as part of the NaaS solution test with WLCs (5520/8540).

PROCESS

Configuring C3850 Converged Access Switch with Wired and Wireless Support

1. Configure a flow record
2. Configure a flow exporter
3. Configure a flow monitor
4. Apply flow monitor to a support port type(s)
5. Switch configuration to quarantine wireless clients

Cisco Catalyst 3850 supports both ingress and egress FnF on all ports of the switch at line rate. Switch raw scalability is up to 24K-cached flows. Cisco Catalyst 3850 supports NetFlow Version 9, with IPv4, IPv6, Layer 2 flows, and sampled NetFlow. TCP flags are also exported as part of the flow information. When Cisco Catalyst 3850 switches are stacked together, each individual stack member exports its own flows to the collector.

Cisco Catalyst 3850 supports up to 16 flow monitors with eight different collectors simultaneously per flow monitor. Microflow policing is supported only for wireless clients.

The FnF feature on the Cisco Catalyst 3850 is enabled on the IP base version and earlier.

Procedure 1 Configure a flow record

Connect to the console of the switch and, in configuration mode, enter the appropriate commands in order to enable ingress and/or egress flow.

Option 1: Enable Ingress Flow

```
flow record FLOW-RECORD1-IN
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
```

Tech Tip

The **match interface output** and **collect interface input** cannot be configured in the ingress flow record. Also both **interface input** and **interface output** in the same flow record are not supported. Only configure one interface direction in one flow record (match or collect).

Option 2: Enable Egress Flow

```
flow record FLOW-RECORD1-OUT
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
```

Tech Tip

The match interface input and collect interface output cannot be configured in the egress flow record.

In the above flow records (Ingress and Egress), there are two statements involving TrustSec Security Groups Tags (SGTs).

```
match flow cts source group-tag
match flow cts destination group-tag
```

The statements ensure that any security group classification known to the switch or present on the wire is exported in the flow record. If you don't plan to enable TrustSec to support NaaE, you can remove these two fields.

Tech Tip

The ability to monitor the security group in a NetFlow record first became available on the 3850/3650 in IOS XE version 3.6.4.

Procedure 2 Configure a flow exporter

Connect to the console and, in configuration mode, enter the following commands.

The NetFlow standard is UDP port 2055.

```
flow exporter FLOW-COLLECTOR1
 destination 10.4.48.70
 transport udp 2055
```

Tech Tip

The C3850 switch can supports up to eight different exporters (collectors) simultaneously per flow monitor.

Procedure 3 Configure a flow monitor

Connect to the console and, in configuration mode, enter the following commands to enable ingress and/or egress flow.

Option 1: Ingress Flow

```
flow monitor FLOW-MONITOR1-IN
 exporter FLOW-COLLECTOR1
 cache timeout active 60
 record FLOW-RECORD1-IN
```

Option 2: Egress Flow

```
flow monitor FLOW-MONITOR1-OUT
 exporter FLOW-COLLECTOR1
 cache timeout active 60
 record FLOW-RECORD1-OUT
```

Procedure 4 Apply flow monitor to a support port type(s)

Connect to the console and, in configuration mode, enter the appropriate commands.

If you plan to quarantine end clients from Stealthwatch, make sure to enable Change of Authorization (CoA) on the Catalyst 3850 switch, which forces the client to re-authenticate and assign appropriate policy. CoA being disabled on the switch may cause an error as a result of ISE returning a RADIUS_FAIL message to Stealthwatch because it was unsuccessful in completing CoA. For information about configuring CoA on a 3850 switch, see Configuring CoA on the Switch.

Option 1: Wired Interface

```
interface GigabitEthernet1/0/1
 description Wired Client in Converged Vlan
 switchport access vlan 10
 switchport mode access
 ip flow monitor FLOW-MONITOR1-IN input
 ip flow monitor FLOW-MONITOR1-OUT output
 load-interval 30
 no shutdown
```

Option 2: VLAN Interface

```
vlan configuration 100
 ip flow monitor FLOW-MONITOR1-IN input
 ip flow monitor FLOW-MONITOR1-OUT output
```

Tech Tip

VLAN 100 is the client VLAN and not the AP Management VLAN. You don't need to configure flow-monitor on the AP Management VLAN.

Option 3: Wireless Interface

```
wlan CAMPUS-SSID-01 1 CAMPUS-SSID-01
 client vlan 100
 ip flow monitor FLOW-MONITOR1-IN input
 ip flow monitor FLOW-MONITOR1-OUT output
 no shutdown
```

NetFlow is now installed on the Catalyst 3850 switch.

Procedure 5 Switch configuration to quarantine wireless clients

Next, you allow SMC to be able to quarantine wireless clients.

This procedure assumes that you already have RADIUS properly configured. If not, see Campus 802.1X Authentication Technology Design Guide.

Step 1: Generate start and stop accounting records.

```
aaa accounting network default start-stop group <radius-server-group-name>
```

Example aaa Configuration

```
aaa authentication dot1x default group ISE_GROUP
aaa authorization network default group ISE_GROUP
aaa authorization configuration default group ISE_GROUP
aaa accounting dot1x default start-stop group ISE_GROUP
aaa accounting network default start-stop group ISE_GROUP
```

Step 2: Enable accounting configuration on the WLAN to send CoA messages from the radius server to quarantine the clients.

```
 accounting-list default
```

Example aaa Configuration

```
wlan CAMPUS-SSID-01 1 CAMPUS-SSID-01
 aaa-override
 accounting-list default
 client vlan 100
 ip flow monitor FLOW-MONITOR1-IN input
 ip flow monitor FLOW-MONITOR1-OUT output
 nac
 security dot1x authentication-list default
 no shutdown
```

PROCESS

Configuring NetFlow on WLC

1. Configure a flow exporter
2. Configure a flow monitor
3. Applying a flow monitor to a WLAN

For Wireless LAN Controller (WLC), you need to configure only two components:

- **NetFlow Exporter–**Network entity that exports the template with the IP traffic information. The WLC controller acts as an exporter.
- **NetFlow Collector–**Entity that collects all the IP traffic information from various NetFlow exporters.

Tech Tip

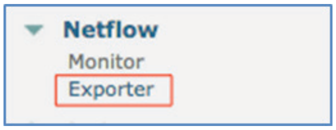
Cisco Wireless Controller does not support IPv6 address as Exporter for NetFlow. For more information, see Cisco Wireless Controller Configuration Guide, Release 8.2.

Procedure 1 Configure a flow exporter

Step 1: Browse and login to the 5520 or 8540 WLC (example: wlc.cisco.local).

Step 2: In the top right corner, click **Advanced**.

Step 3: On the Wireless tab, in the left navigation pane, expand NetFlow, and then click **Exporter**.



Step 4: Click **New**.

Step 5: Enter the following. Even though it's asking you to enter the Exporter IP and port number, you must enter the Flow Collector IP and port.

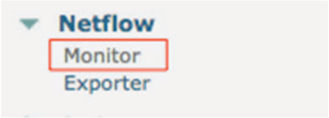
- Exporter name: **Netflow-Collector**
- Exporter IP: **10.4.48.70** (Enter your SW Flow Collector IP Addr.)
- Port number: **2055** (by default, this is UDP 2055)

Step 6: Click **Apply**.

Step 7: Click **Save Configuration**.

Procedure 2 Configure a flow monitor

Step 1: Back on the Wireless tab, in the left navigation pane, expand Netflow, and then and click **Monitor**.



Step 2: Click **New**.

Step 3: Enter the monitor name (example: NetFlow-Monitor).

Step 4: Click **Apply**.

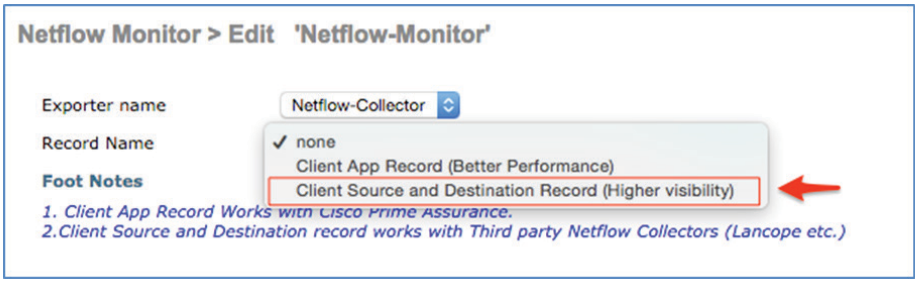
Step 5: On the Monitor List page, click the newly created Monitor (example: NetFlow-Monitor).

Step 6: In the **Exporter name** list, select **Netflow-Collector**.

Tech Tip

For WLC you don't have a separate step to configure Flow Record. The configuration of Flow Record is part of Flow Monitor in the above steps.

Step 7: In the **Record Name** list, select **Client Source and Destination Record**.



Netflow Monitor > Edit 'Netflow-Monitor'

Exporter name: Netflow-Collector

Record Name:
- ✓ none
- Client App Record (Better Performance)
- Client Source and Destination Record (Higher visibility)

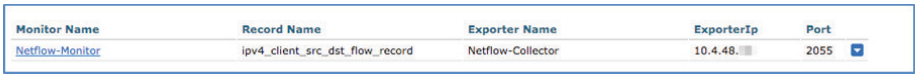
Foot Notes

1. Client App Record Works with Cisco Prime Assurance.
2.Client Source and Destination record works with Third party Netflow Collectors (Lancope etc.)

Tech Tip

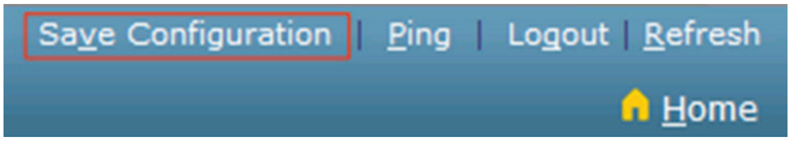
The Client Source and Destination Record (Higher Visibility) record name was added starting with WLC 8.2. You must use this record name with Stealthwatch in order to leverage the enhanced features of NetFlow v9.

Step 8: Click **Apply.** The Monitor List page reflects the following details.



Monitor Name	Record Name	Exporter Name	ExporterIp	Port
Netflow-Monitor	ipv4_client_src_dst_flow_record	Netflow-Collector	10.4.48.[redacted]	2055

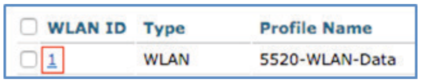
Step 9: Click **Save Configuration**.



Procedure 3 Applying a flow monitor to a WLAN

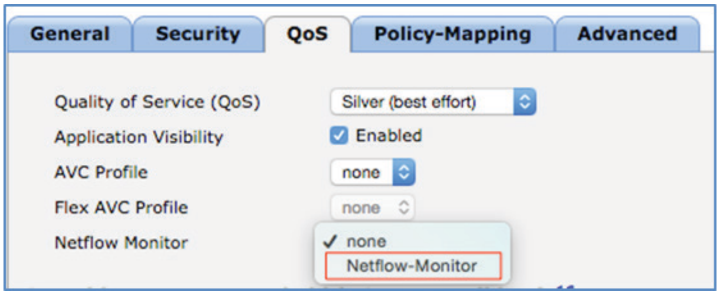
Associate a NetFlow Monitor to a WLAN.

Step 1: Navigate to WLANs, and then click the WLAN ID to open the WLAN where you will configure NetFlow.



☐ WLAN ID	Type	Profile Name
☐ 1	WLAN	5520-WLAN-Data

Step 2: On the QoS tab, in the **Netflow Monitor** list, select **Netflow-Monitor**, which you created in "Configure a flow monitor."



Quality of Service (QoS) Silver (best effort)

Application Visibility ☑ Enabled

AVC Profile none

Flex AVC Profile none

Netflow Monitor ✓ none / Netflow-Monitor

Step 3: Click **Apply**.

Tech Tip

AVC is enabled by default when NetFlow is enabled on WLC 5520 or 8540.

Step 4: On WLC, make sure CoA is enabled. It is important when quarantining or unquarantining a device from Stealthwatch. Login to WLC, navigate to **Security > Radius > Authentication,** select the ISE Node to verify and from the **Support for CoA** list, select **Enabled**. Click **Apply**.

Step 5: Enable Interim Updates by navigating to WLANs tab. Select the WLAN ID and navigate to **Security > AAA Servers**, and in the RADIUS Server Accounting section, check the box next to Interim Update and change the internal to 180. Click **Apply**.

Step 6: Click **Save Configuration**.

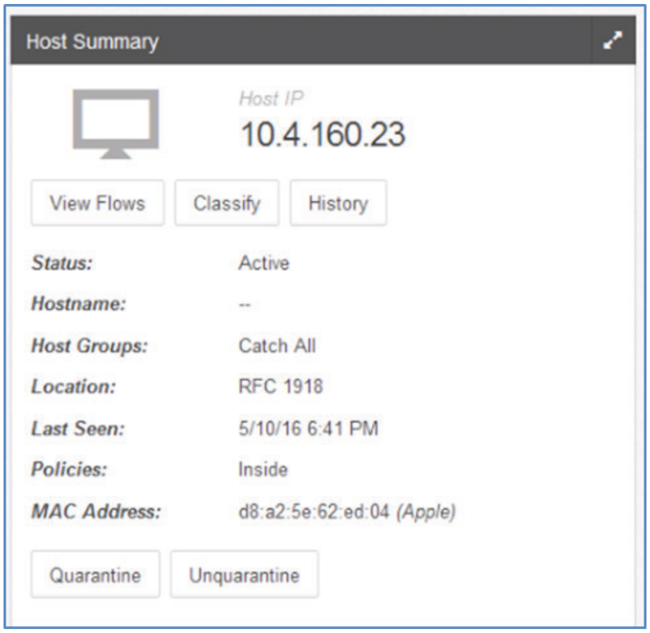
Now you have completed required tasks to enable NetFlow on 5520/8540 Switch.

Tech Tip

Stealthwatch 6.7.1 doesn't support WLAN as a flow interface (unable to consume SSID/AP MAC addresses). Instead it reports the physical interface of the switch, which causes the interface to report invalid utilization. In terms of flows, Stealthwatch won't represent wireless flows differently. It appears similar to wired flows. This is expected to be resolved in a future release.

Enabling Quarantine

In Procedure 3, “Verify pxGrid services and switch to Endpoint Protection Services,” you subscribed the SMC (Stealthwatch) to the EPS Group in ISE. Until you create an authorization policy in ISE, clicking the **Quarantine** or **Unquarantine** button from the SMC dashboard (under Networks > Host > Host-IP) will have no effect.



Host IP
10.4.160.23

Status: Active
Hostname: --
Host Groups: Catch All
Location: RFC 1918
Last Seen: 5/10/16 6:41 PM
Policies: Inside
MAC Address: d8:a2:5e:62:ed:04 *(Apple)*

Tech Tip

Due to an open bug in Stealthwatch 6.7.1, flows status is reported as Inactive, even though it’s Active, under the Host Summary. This has been fixed in 6.6.3 and 6.7.3.

Next, you configure an Authorization Policy that takes advantage of the quarantine attribute in order to assign a suspicious host to the Quarantine_System SGT and also define segmentation policy for the Quarantine_System SGT.

Tech Tip

Based on the specific use-case, you can quarantine traffic to a specific server in the data center. This example assumes that TrustSec has been enabled on the network device in ISE. For example, a Finance_Server SGT is configured. For step-by-step instructions about configuring TrustSec in the User-to-DC use case, see User-to-Data-Center Access Control Using TrustSec Deployment Guide.

PROCESS

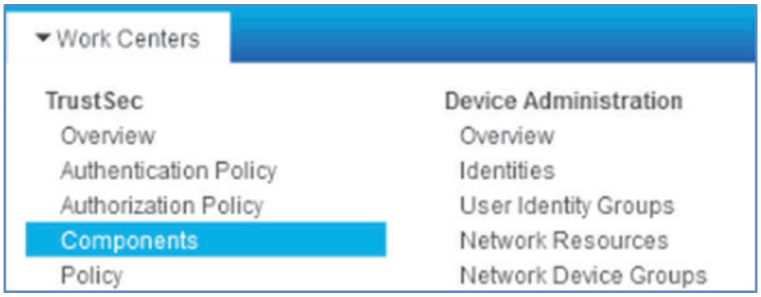
Quarantining SGT

1. Configure Quarantine SGT
2. Configure authorization policy for Quarantine SGT

Procedure 1 Configure Quarantine SGT

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to **Work Centers > TrustSec > Components**.



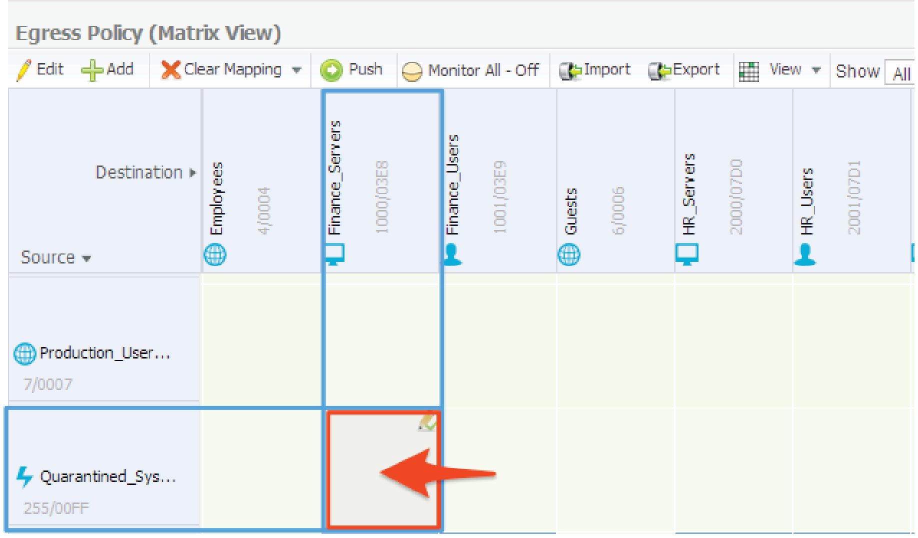
Step 3: Under Security Groups, verify the following SGTs have been created (tag number may vary).

- Employee (4/0004)
- Quarantined_Systems (255/00FF) SGT
- Finance_Server (1000/03E8)
- HR_Server (2000/07D0)

Step 4: Under Security Group ACLs, verifyfor a Deny_All ACL that includes “deny ip log” has been created.

Step 5: Navigate to **Work Centers > TrustSec > Policy**, expand **Egress Policy**, and then click **Matrix**.

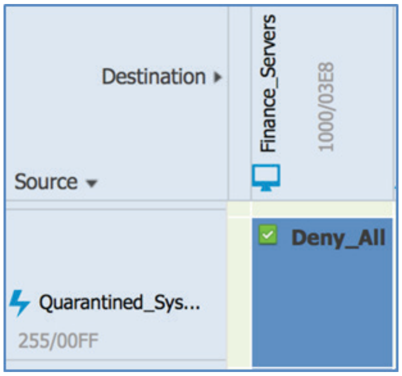
Step 6: From the Matrix setting, double-click the box intersecting the source **Quarantine_System** and the destination **Finance_Servers**.



Step 7: Select the **Deny_All** ACL and make sure Status is Enabled.

Step 8: Click **Save**.

Step 9: Ensure the policy Matrix reflects the new policy, **Deny_All**.



Tech Tip

The top right of the menu bar will now show one notification, indicating the new TrustSec policy changes are not yet pushed to the switch.

Step 10: Click **Push**. The new policy change applies on the enforcer switch (example: Nexus 7000 in Datacenter).

Procedure 2 Configure authorization policy for Quarantine SGT

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to **Policy > Authorization Policy**.

Step 3: In the Authorization Policy section, expand **Exceptions**.

Step 4: Click **Create a New Rule**.

Tech Tip

The ANC (Adaptive Network Control—Earlier, Endpoint Protection Service-EPS) is enabled by default in Cisco ISE 2.0.

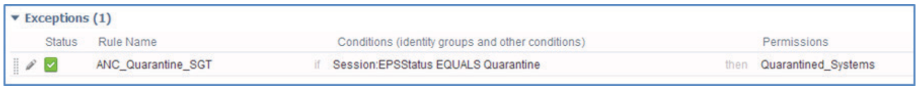
Step 5: Configure the authorization policy with following settings:

Rule Name: **ANC_Quarantine_SGT**

Conditions: **Create New Condition (Advanced Option) > Session > EPSStatus > (Equals) 'Quarantine'**

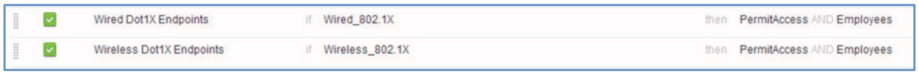
Permissions: **Security Group > Quarantine_Systems**

Step 6: Click **Done**, and then click **Save.** Under the Exceptions condition, the configured authorization policies look like the following.



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	ANC_Quarantine_SGT	if	Session:EPSStatus EQUALS Quarantine	then	Quarantined_Systems

Step 7: You may also verify the Standard condition (for example, 802.1X policy with Employee SGT) that will be the initial tag assigned to the corporate user upon login.



✓	Wired Dot1X Endpoints	if	Wired_802.1X	then	PermitAccess AND Employees
✓	Wireless Dot1X Endpoints	if	Wireless_802.1X	then	PermitAccess AND Employees

PROCESS

Quarantining VLAN

1. Create an authorization profile
2. Configure an authorization policy

Procedure 1 Create an authorization profile

Step 1: Navigate to **Policy** > **Policy Elements** > **Results**.

Step 2: From left pane, select **Authorization** > **Authorization Profiles**.

Step 3: Expand Common Tasks, and then select **VLAN**.

Step 4: Enter the **Quarantine VLAN ID** (for example 666). Leave the default Tag ID set to 1.

Step 5: Click **Add**, and then click **Save**.

Procedure 2 Configure an authorization policy

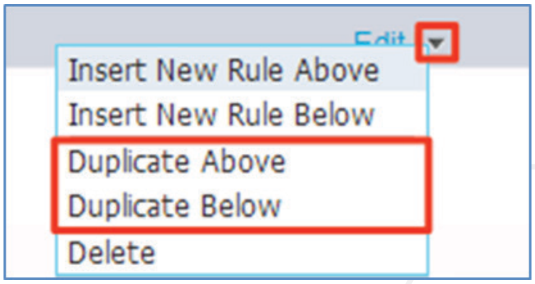
Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to **Policy** > **Authorization Policy**.

Step 3: In the Authorization Policy section, expand **Exception**.

Step 4: Click **Create a New Rule**.

Step 5: If you have already created the **ANC_Quarantine_SGT** in the previous steps, then you will have to duplicate the policy and edit. To do so, click the triangle and select **Duplicate Above** or **Duplicate Below**.



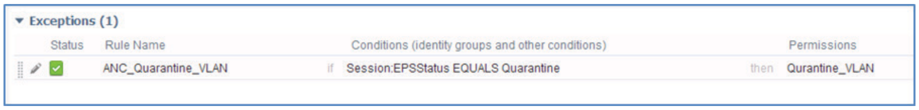
Step 6: Edit and configure the authorization policy with following settings:

Rule Name: **ANC_Quarantine_VLAN**

Conditions: **Create New Condition (Advanced Option) > Session > EPSStatus > (Equals) 'Quarantine'**

Permissions: **Standard > Quarantine_VLAN**

Step 7: Click **Done**, and then click **Save**. Under the Exceptions condition, the configured authorization policies look like the following.



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	ANC_Quarantine_VLAN	if	Session:EPSStatus EQUALS Quarantine	then	Qurantine_VLAN

PROCESS

Verifying and Testing

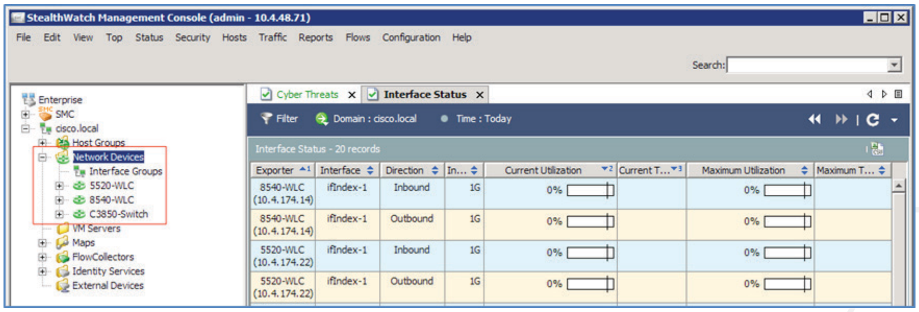
1. Perform Stealthwatch communication check with network devices
2. Test network visibility

In this process, you verify the NaaS deployment. If Quarantine is enabled, also test the containment (Quarantine) feature from the Stealthwatch Web GUI.

Procedure 1 Perform Stealthwatch communication check with network devices

Step 1: Launch the Stealthwatch Java client and log in.

Step 2: From left pane, navigate to **Domain Name** (example: cisco.local) **> Host Groups > Network Devices**, and make sure all the NetFlow-enabled Network Access Devices are listed.



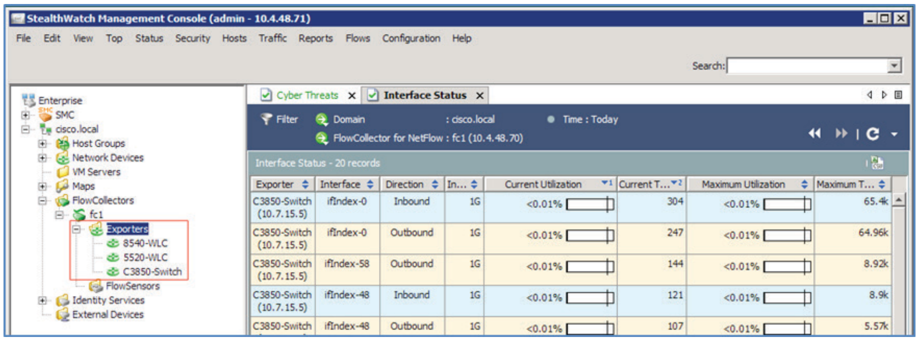
Interface Status - 20 records

Exporter	Interface	Direction	In...	Current Utilization	Current T...	Maximum Utilization	Maximum T...
8540-WLC (10.4.174.14)	ifIndex-1	Inbound	1G	0%		0%	
8540-WLC (10.4.174.14)	ifIndex-1	Outbound	1G	0%		0%	
5520-WLC (10.4.174.22)	ifIndex-1	Inbound	1G	0%		0%	
5520-WLC (10.4.174.22)	ifIndex-1	Outbound	1G	0%		0%	

Tech Tip

Under **Network Devices**, a device will only be listed if NetFlow is configured properly. You cannot manually add a network device from the Stealthwatch client.

Step 3: From the left pane, expand **FlowCollectors** and make sure all the NetFlow enabled Network Access Devices are listed.



Domain : cisco.local
Time : Today
FlowCollector for NetFlow : fc1 (10.4.48.70)

Interface Status - 20 records

Exporter	Interface	Direction	In...	Current Utilization	Current T...	Maximum Utilization	Maximum T...
C3850-Switch (10.7.15.5)	ifIndex-0	Inbound	1G	<0.01%	304	<0.01%	65.4k
C3850-Switch (10.7.15.5)	ifIndex-0	Outbound	1G	<0.01%	247	<0.01%	64.96k
C3850-Switch (10.7.15.5)	ifIndex-58	Outbound	1G	<0.01%	144	<0.01%	8.92k
C3850-Switch (10.7.15.5)	ifIndex-48	Inbound	1G	<0.01%	121	<0.01%	8.9k
C3850-Switch	ifIndex-48	Outbound	1G	<0.01%	107	<0.01%	5.57k

Tech Tip

Under **FlowCollectors > fc1 > Exporters**, if a device is not listed, manually add all the NetFlow enabled devices as an Exporter within the Stealthwatch client. Right-click **Exporters,** select **Configuration > Add Exporters**, enter the IP address and name of the device, and then click **OK**.

Step 4: To verify NetFlow data collection, expand **FlowCollectors**, right-click your Flow Collector (example: fc1), and navigate to **Status > NetFlow Collection Status.** Under **Current NetFlow Traffic (bps)**, check the counters increment.

Step 5: Right-click the **Flow Collection Status** table header, and then check **Longest Duration Export** to enable the column to correlate the time duration for the flows.

Tech Tip

Here are a few **show** and **clear** commands to keep handy for troubleshooting or viewing your NetFlow data from the switch. The below validation commands are for ingress (IN) flows. You may repeat the commands for in egress (OUT) traffic.

Commands to display NetFlow data:

```
show flow record FLOW-RECORD1-IN
show flow monitor FLOW-MONITOR1-IN statistics
show flow monitor FLOW-MONITOR1-IN cache
show flow exporter FLOW-COLLECTOR1-IN statistics
```

Commands to reset NetFlow data:

```
clear flow record FLOW-RECORD1-IN
clear flow monitor FLOW-MONITOR1-IN statistics
clear flow monitor FLOW-MONITOR1-IN cache
clear flow exporter FLOW-COLLECTOR1-IN statistics
```

Procedure 2 Test network visibility

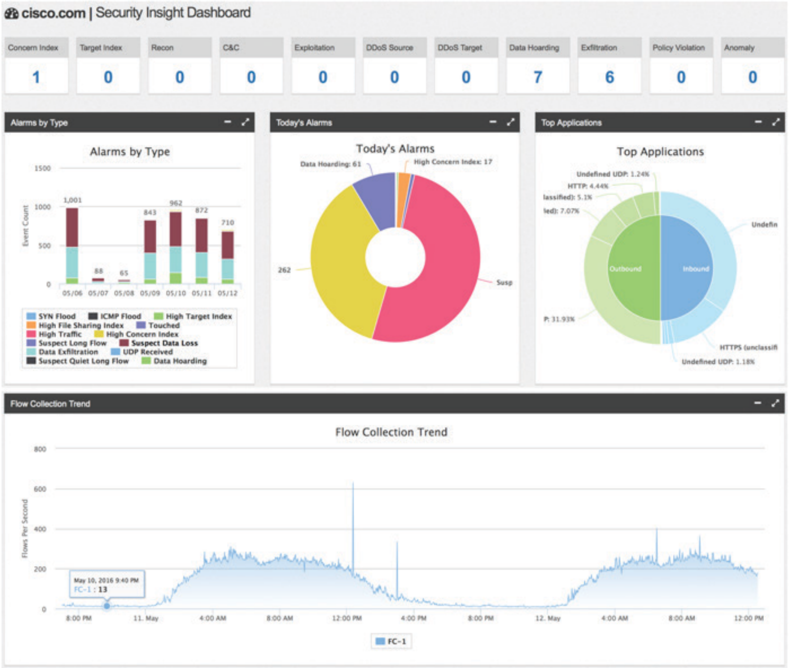
Step 1: Connect a wired or wireless client (example: iPad, PC or VM) to the NetFlow-enabled Network Device (example: 3850 switch, 8540 or 5520 WLC) Interface (example: Physical, or WLAN).

Step 2: Log in to ISE (example: ise.cisco.local).

Step 3: Navigate to **Operations > Radius Livelog**, and based on the Authentication method (example: 802.1X), make sure the user connects successfully and assigned appropriate SGT (example: Employee).

Step 4: Log in to the Stealthwatch web-client (example: smc.cisco.local).

Figure 8 Typical Stealthwatch dashboard

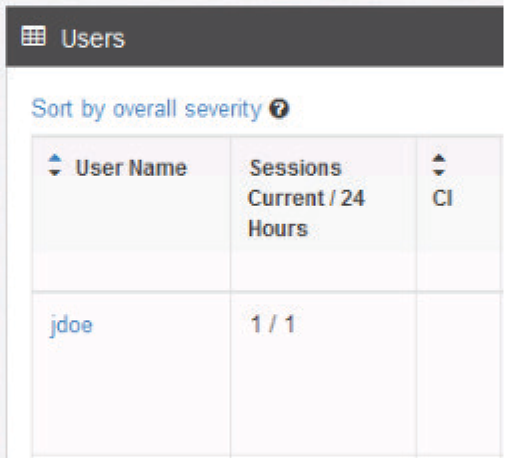


Tech Tip

In Stealthwatch 6.7.1, SMC Web GUI Dashboard, the Top Applications chart doesn't show application names and it cannot be customized to show NBAR granularity at the moment.

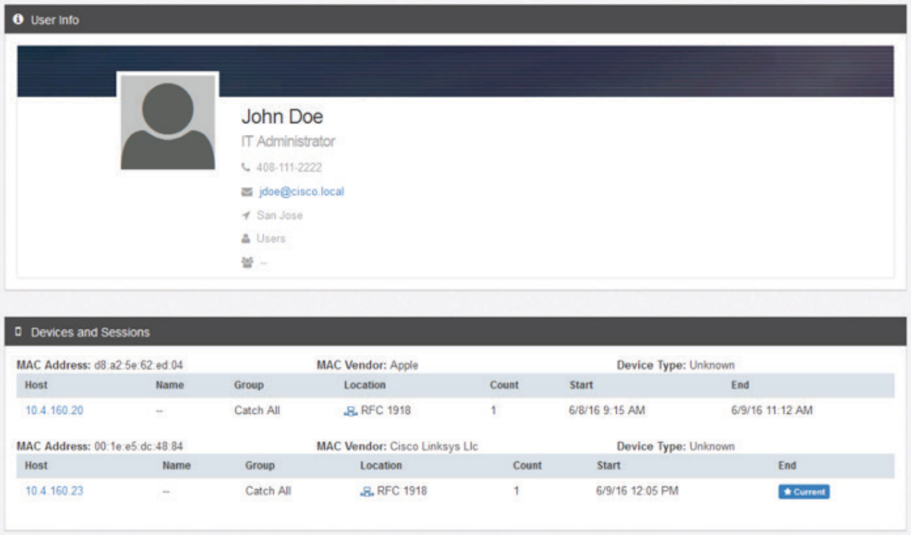
The above figure represents a typical Stealthwatch dashboard based on an active flow collection for a longer duration. A newly installed setup will not be able to populate all the widgets as shown above. Refer to Stealthwatch documentation on creating **Custom Events**, which are security policies to trigger Alarms.

Step 5: Navigate to **Network > Users** and verify the authenticated username is shown.



User Name	Sessions Current / 24 Hours	CI
jdoe	1 / 1	

Step 6: Click a user name with suspicious activity to reveal more details, as shown below.



John Doe
IT Administrator
408-111-2222
jdoe@cisco.local
San Jose
Users
--

MAC Address: d8:a2:5e:62:ed:04 **MAC Vendor:** Apple **Device Type:** Unknown

Host	Name	Group	Location	Count	Start	End
10.4.160.20	--	Catch All	RFC 1918	1	6/8/16 9:15 AM	6/9/16 11:12 AM

MAC Address: 00:1e:e5:dc:48:84 **MAC Vendor:** Cisco Linksys Llc **Device Type:** Unknown

Host	Name	Group	Location	Count	Start	End
10.4.160.23	--	Catch All	RFC 1918	1	6/9/16 12:05 PM	★ Current

Tech Tip

User information populates based on information provided by Active Directory, and the Devices and Sessions table lists all of the recent devices used, including active clients. Select a device IP address to further investigate.

Step 7: Under Host Summary, click the **Quarantine** button in order to mitigate a suspicious device.

Tech Tip

The Quarantine or Unquarantine button functions only if the MAC Address field is populated under Host Summary.

When you click Quarantine or Unquarantine from Stealthwatch, you may see a success or failure message. The result could actually be the opposite of what the message indicates, due to the response delay from ISE to Stealthwatch.

The failure message can also occur if you mandate that the client re-authenticate (ISE will timeout and send a fail message over the API), but in fact the quarantine was successful (that is, the EPS status was set to true and when the user logs in again, the device is quarantined).

Step 8: After the device can safely connect to the network, click **Unquarantine**.

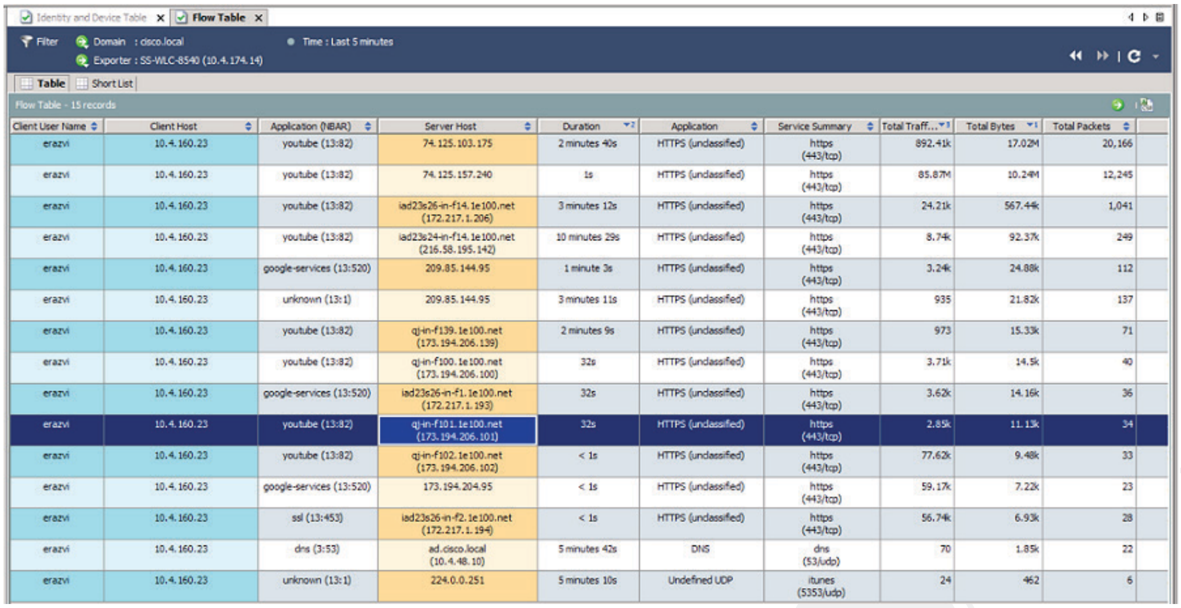
Step 9: Under Host Summary, click **View Flows** and optionally edit the parameters. Click **Review Query**, and then click **Run** to start Flow Query and show the result.

Step 10: Click **Launch SMC**. The Java client opens.

Tech Tip

In Stealthwatch 6.7.1, visibility into applications is limited. Many TCP/UDP applications are tagged as “Undefined TCP/Undefined UDP,” causing finer granularity to be lost within Apps/Services category. This is in spite of NBAR classification being active. This is expected to be fixed for the 6.8 release.

Step 11: To test application visibility, from the left pane, expand **FlowCollectors > fc1 > Exporters**, right-click a network device (example: WLC 5520/8540), and navigate to **Flows > Flow Table**. If AVC is enabled, adding the Application (NBAR) column displays the application/website (example: YouTube) being browsed.



Domain : cisco.local

Exporter : SS-WLC-8540 (10.4.174.14)

Time : Last 5 minutes

Flow Table - 15 records

Client User Name	Client Host	Application (NBAR)	Server Host	Duration	Application	Service Summary	Total Traff...	Total Bytes	Total Packets
erazvi	10.4.160.23	youtube (13:82)	74.125.103.175	2 minutes 40s	HTTPS (unclassified)	https (443/tcp)	892.41k	17.02M	20,166
erazvi	10.4.160.23	youtube (13:82)	74.125.157.240	1s	HTTPS (unclassified)	https (443/tcp)	85.87M	10.24M	12,245
erazvi	10.4.160.23	youtube (13:82)	iad23s26-in-f14.1e100.net (172.217.1.206)	3 minutes 12s	HTTPS (unclassified)	https (443/tcp)	24.21k	567.44k	1,041
erazvi	10.4.160.23	youtube (13:82)	iad23s24-in-f14.1e100.net (216.58.195.142)	10 minutes 29s	HTTPS (unclassified)	https (443/tcp)	8.74k	92.37k	249
erazvi	10.4.160.23	google-services (13:520)	209.85.144.95	1 minute 3s	HTTPS (unclassified)	https (443/tcp)	3.24k	24.88k	112
erazvi	10.4.160.23	unknown (13:1)	209.85.144.95	3 minutes 11s	HTTPS (unclassified)	https (443/tcp)	935	21.82k	137
erazvi	10.4.160.23	youtube (13:82)	qj-in-f139.1e100.net (173.194.206.139)	2 minutes 9s	HTTPS (unclassified)	https (443/tcp)	973	15.33k	71
erazvi	10.4.160.23	youtube (13:82)	qj-in-f100.1e100.net (173.194.206.100)	32s	HTTPS (unclassified)	https (443/tcp)	3.71k	14.5k	40
erazvi	10.4.160.23	google-services (13:520)	iad23s26-in-f1.1e100.net (172.217.1.193)	32s	HTTPS (unclassified)	https (443/tcp)	3.62k	14.16k	36
erazvi	10.4.160.23	youtube (13:82)	qj-in-f101.1e100.net (173.194.206.101)	32s	HTTPS (unclassified)	https (443/tcp)	2.85k	11.13k	34
erazvi	10.4.160.23	youtube (13:82)	qj-in-f102.1e100.net (173.194.206.102)	< 1s	HTTPS (unclassified)	https (443/tcp)	77.62k	9.48k	33
erazvi	10.4.160.23	google-services (13:520)	173.194.204.95	< 1s	HTTPS (unclassified)	https (443/tcp)	59.17k	7.22k	23
erazvi	10.4.160.23	ssl (13:453)	iad23s26-in-f2.1e100.net (172.217.1.194)	< 1s	HTTPS (unclassified)	https (443/tcp)	56.74k	6.93k	28
erazvi	10.4.160.23	dns (3:53)	ad.cisco.local (10.4.48.10)	5 minutes 42s	DNS	dns (53/udp)	70	1.85k	22
erazvi	10.4.160.23	unknown (13:1)	224.0.0.251	5 minutes 10s	Undefined UDP	itunes (5353/udp)	24	462	6

You have now successfully deployed and tested the NaaS solution.

For more information about using Stealthwatch, refer to the Stealthwatch Management Console User’s Guide from the Stealthwatch download center.

Appendix A: Product List

The following products and software versions have been validated for CVD.

STEALTHWATCH

Functional Area	Product	Part Numbers	Software Version
Cisco FlowCollector	StealthWatch FlowCollector for NetFlow Virtual Edition	L-LC-FC-NF-VE-K9	6.7.1
Cisco SMC Server	StealthWatch Management Console Virtual Edition	L-LC-SMC-VE-K9	6.7.1

IDENTITY MANAGEMENT

Functional Area	Product	Part Numbers	Software Version
Cisco ISE Server	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	2.0.0.306 Cumulative Patch 2
	Cisco Identity Services Engine 10000 EndPoint Base License	L-ISE-BSE-10K=	
	Cisco Identity Services Engine 5000 EndPoint Base License	L-ISE-BSE-5K=	
	Cisco Identity Services Engine 3500 EndPoint Base License	L-ISE-BSE-3500=	
	Cisco Identity Services Engine 2500 EndPoint Base License	L-ISE-BSE-2500=	
	Cisco Identity Services Engine 1500 EndPoint Base License	L-ISE-BSE-1500=	
	Cisco Identity Services Engine 1000 EndPoint Base License	L-ISE-BSE-1K=	
	Cisco Identity Services Engine 500 EndPoint Base License	L-ISE-BSE-500=	
	Cisco Identity Services Engine 250 EndPoint Base License	L-ISE-BSE-250=	
	Cisco Identity Services Engine 100 EndPoint Base License	L-ISE-BSE-100=	
	Cisco ISE 10K Endpoint Plus Subscription License	L-ISE-PLS-S-10K=	
	Cisco ISE 5K Endpoint Plus Subscription License	L-ISE-PLS-S-5K=	
	Cisco ISE 3500 Endpoint Plus Subscription License	L-ISE-PLS-S-3500=	
	Cisco ISE 2500 Endpoint Plus Subscription License	L-ISE-PLS-S-2500=	
	Cisco ISE 1500 Endpoint Plus Subscription License	L-ISE-PLS-S-1500=	
	Cisco ISE 1K Endpoint Plus Subscription License	L-ISE-PLS-S-1K=	
	Cisco ISE 500 Endpoint Plus Subscription License	L-ISE-PLS-S-500=	
	Cisco ISE 250 Endpoint Plus Subscription License	L-ISE-PLS-S-250=	
	Cisco ISE 100 Endpoint Plus Subscription License	L-ISE-PLS-S-100=	

LAN ACCESS LAYER

Functional Area	Product	Part Numbers	Software Version
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.6.4.E(15.2.2E4) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	

WIRELESS LAN CONTROLLERS

Functional Area	Product	Part Numbers	Software Version
On Site Controller	Cisco 5520 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5520-50-K9	8.2.100.0
	Cisco 5520 Wireless Controller 100 AP License	LIC-CTS5520-100A	
	Cisco 5520 Wireless Controller 50 AP License	LIC-CTS5520-50A	
	Cisco 5520 Wireless Controller 1 AP Adder License	LIC-CT5520-1A	
On Site Controller	Cisco 8540 Wireless Controller supporting 1000 access points	AIR-CT8540-1K-K9	8.2.100.0
	Cisco 8540 Wireless Controller	AIR-CT8540-K9	
	Cisco 8540 Wireless Controller 1 AP Adder License	LIC-CT8540-1A	

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2016 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)