# Table of Contents

About This Document ..................................................................................................................... 1

Cisco TrustSec Overview ................................................................................................................. 2

Use Cases ....................................................................................................................................... 3

- Retail: Segmentation for PCI Compliance .......................................................................................... 3
- Healthcare: Securing Access to Medical Devices and Electronic Health Records for HIPAA Compliance ................................................................. 4
- Finance: Bank Branch Needs to Provide Differentiated Access for the Various Services at a Remote Site ........................................................................ 6
- Line of Business Access Control in Large Enterprises ........................................................................ 7
- Design Overview ........................................................................................................................................................... 10

Deployment Details ........................................................................................................................ 12

- Deploying ISE ................................................................................................................................................................ 13
- Enabling Wired Authentication ...................................................................................................................... 34
- Enabling Wireless Authentication ..................................................................................................................... 38
- Assigning SGTs to Servers ............................................................................................................................... 44
- Configuring SGT Propagation ......................................................................................................................... 47
- Enabling Enforcement in the DC .................................................................................................................... 71

Appendix A: Product List ............................................................................................................... 77
About This Document

This document describes how Cisco TrustSec provides access control for user to data center ("north to south") traffic for wired and wireless users. Cisco TrustSec provides software-defined segmentation and enables role-based security policy.

Tech Tip

For more information about Cisco TrustSec, go to:
http://www.cisco.com/go/trustsec
Cisco TrustSec Overview

The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not IP address, enabling policy change without network redesign. A centralized policy management platform gathers advanced contextual data about who and what is accessing your network, uses security group tags (SGTs) to define roles and access rights and then pushes the associated policy to your TrustSec-enabled network devices, such as switches, routers, and security equipment. This provides better visibility through richer contextual information and allows an organization to be better able to detect threats and accelerate remediation, reducing the impact and costs associated with a potential breach.

Cisco TrustSec technology is embedded in Cisco switches, routers, and firewalls and is defined in three phases: classification, propagation, and enforcement. When the user’s traffic enters the network, the traffic is classified based on the results of authentication, such as 802.1X, MAC authentication bypass, or web authentication. After the user’s traffic is classified, Cisco switches and routers then propagate the traffic automatically, without any intervention by the network operator until it hits an enforcement point, which can be a Cisco firewall, router, or switch. Based on the classification, the enforcement device determines if the user’s traffic should be allowed or denied.

Figure 1  Cisco TrustSec phases: classification, propagation, and enforcement
Use Cases

RETAIL: SEGMENTATION FOR PCI COMPLIANCE

Business Problem
A retail chain is required to comply with Payment Card Industry (PCI) standards where all devices that process credit-card information are in a network that is segmented from other devices.

Solution
The PCI devices are tagged by the switch or router at the store and provided access to the payment servers in the data center, which is enforced at the data center by a data center switch or the data center firewall. The devices on the network that aren’t used for processing payment information get an appropriate tag that prevents them from accessing the payment servers but allows them access to shared services provided in the data center.

Figure 2  TrustSec for PCI compliance

![Diagram of TrustSec for PCI compliance]

- Data Center
  - Payment Servers
  - Shared Services
- PCI Zone
  - Local Servers
- Store WAN DMVPN
- ISE
- Manager PC
- POS
- Associate
- Voice
- Store 1
- Store 2
HEALTHCARE: SECURING ACCESS TO MEDICAL DEVICES AND ELECTRONIC HEALTH RECORDS FOR HIPAA COMPLIANCE

Business Problem
A hospital needs to limit access to electronic health records in order to comply with the Health Insurance Portability and Accountability Act (HIPAA).

Figure 3 TrustSec for HIPAA compliance
Use Cases

The hospital also needs to isolate medical devices used for patient care so that only authorized users, devices and servers have access to these medical devices.

Figure 4 TrustSec for medical device segmentation

Solution

Medical professionals use an authorized workstation in order to gain access to the electronic health records. The user authenticates to Cisco Identity Services Engine (ISE) and the device is verified to make sure it is authorized for access to the health records. The switch or wireless LAN controller (WLC) tags (with an SGT) the traffic from this workstation. The policy is enforced on the DC firewall with a Cisco Security Group Firewall (SGFW) that allows access to the electronic health records server only to those devices and users that are authorized, and all other devices and users are denied access.

SGTs are applied to authenticated users of medical devices and servers in order to explicitly allow access for authorized users by using security group access control Lists (SGACLs). Devices and users on the network that don’t receive the SGT assigned are denied access.
FINANCE: BANK BRANCH NEEDS TO PROVIDE DIFFERENTIATED ACCESS FOR THE VARIOUS SERVICES AT A REMOTE SITE

Business Problem
A financial customer requires segmentation of their various services at a remote office. The employee traffic, voice traffic, and server traffic must be in separate networks, as will any guest or bring your own device (BYOD) access. Each individual service must only be given access to the services that are required.

Solution
Each service at the remote site is in its own VLAN. When a device or user accesses the network, ISE authenticates and profiles them. The switch tags the traffic per VLAN, and then the policy is enforced on the remote site router using SGACLs as well as at the DC firewall using SGFW. Corporate traffic is allowed access only to the specific resources required for them. In this case, the employee can access the application server, the phone accesses the communication services, and the remote site server has access only to the database server. The guest or BYOD traffic is given access only to the Internet. With this topology, the VLAN scheme and tagging per VLAN can be replicated at every remote site, making policy configuration simple.

Figure 5 TrustSec for remote site segmentation
LINE OF BUSINESS ACCESS CONTROL IN LARGE ENTERPRISES

Business Problem
New business risk and regulatory concerns require the business to implement security controls for users to the data center and within the data center:

- Users (and devices) should only be allowed to base services and corresponding line of business applications.
- Applications should be segregated by line of business as well as restricted within the line of business.
- Policies are automatically applied for partner/contractors for application and other services.

Solution

Controlling the Services a User Can Access Based on Group Membership
Within the data center, there are specific resources available to different groups of users. For example, there are two servers in the data center, one that only the Finance group can access and another that is only for the Human Resources group. Users identified as members of either group are allowed access to their respective server, and any traffic from any other group is blocked by either the firewall or the data center router.

Figure 6  TrustSec for line-of-business access control
When the user first accesses the network, they authenticate. The switch or the WLC authenticates the user by using Cisco ISE, and the user is assigned a tag. The switch or WLC tags (with the SGT) the traffic from this user. The policy is enforced, based on the SGT, in the data center with an SGACL on the DC router or with an SGFW on the DC firewall.

Permitting Access to Data Center Resources Based on Device Type

An organization may have a BYOD policy that allows employees to use their smartphones and tablets for work. However, some services may not work well on these platforms, or perhaps policy doesn’t allow personal devices access to certain resources. These devices are profiled, classified, and prevented from accessing services not intended for their use.

The user accesses the network with their BYOD device and is prompted for authentication credentials. Upon successful authentication, ISE profiles the device in order to determine the type of device, and the user is assigned a tag based on a combination of user and device type. The WLC tags traffic from the BYOD device and the user is limited to the BYOD server in the data center. This is enforced on the DC router with an SGACL or on the DC firewall with an SGFW.
Providing Differentiated Access to Data Center Resources Based on the User and Location

An organization may want to provide different levels of access to services in the data center, depending on where the user is located. There may be a different policy for users at a remote site that limits what the user can access remotely. This policy could also implement different levels of access per remote site or region.

Figure 8 TrustSec for location-based access control

The remote employee accesses the network and authenticates, and the user is assigned a tag. The switch tags this traffic with the SGT, and this tag information is propagated to the DC firewall, where the policy is enforced with an SGFW.

Ensuring That Devices Are Compliant with Security Policy before Accessing Data Center Resources

To comply with security policy, all devices on the network must meet certain requirements, such as running an antivirus application or a minimum version of an OS. Without meeting the policy, the user is denied access to the data center resources and instead given access to remediation services.
The user accesses the network with a device that does not comply with the security policy. The user authenticates to the network, and Cisco ISE profiles the device and checks for compliance. After the device is determined to be non-compliant, the device is assigned a tag that indicates it is out of compliance and limits access to the remediation service. The policy is enforced with an SGACL, at the access switch or at the DC switch.

**DESIGN OVERVIEW**

Cisco ISE is an identity and access control policy platform that enables organizations to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is a core component of a Cisco TrustSec network. Its architecture allows an organization to gather real-time contextual information from the network, users, and devices to make proactive policy decisions by tying identity into network elements such as access switches, wireless controllers, and VPN gateways.

This deployment uses Cisco ISE as the authentication, authorization, and accounting server for the wired and wireless networks using RADIUS. Cisco ISE acts as a proxy to the existing Active Directory (AD) services to maintain a centralized identity store for all network services.

In addition to authentication, this deployment uses Cisco ISE to profile devices in order to determine the spec-
specific type of devices that are accessing the network. This is done by examining network traffic for certain criteria, based on certain characteristics. Cisco ISE currently has probes for Dynamic Host Configuration Protocol (DHCP), HTTP, RADIUS, Domain Name System (DNS), Simple Network Management Protocol (SNMP) traps and queries, Network Mapper (Nmap) scans, and Cisco IOS NetFlow. To analyze the traffic, the engine can be deployed as an inline policy enforcement device, or the traffic can be forwarded to the engine. As an example, the network infrastructure is configured to send DHCP and Cisco Discovery Protocol (CDP) data via RADIUS to Cisco ISE for analysis. The engine then evaluates the RADIUS data and can identify the device based off of the data in the RADIUS packet. For example, Cisco IP Phones are identified by their DHCP class identifier.

This document builds upon the foundation of the Campus 802.1X Authentication Technology Design Guide where both 802.1X monitor mode and low-impact mode deployments are shown.

The deployment in use will use dynamic classification on the access switches and wireless LAN controllers and assign a tag based on the user’s group assignment in Active Directory. The policy deployed restricts the user’s access to their specific departmental servers in the data center. For example, users in the Finance group can only access the Finance group’s servers. This policy is enforced at the Cisco Nexus 7000 switches and also at the Cisco ASA 5585 cluster in the core of the data center.

To propagate the tags throughout the network, the deployment uses two methods. The first method is using inline tagging in the data plane. The tag is embedded in the Cisco metadata in the Layer 2 header and carried throughout the network. This requires that all infrastructure along the path must support inline tagging. The second is using the SGT Exchange Protocol (SXP), which is a control plane protocol that propagates the IP-to-SGT mapping database from network authentication points such as access layer switches to upstream network devices. SXP is a TCP-based peering protocol and can be used to propagate tags in an environment where all devices do not support inline tagging.

Figure 10  Example network
Deployment Details

The deployment described is based on several design guides that comprise the reference network architecture. Those guides are the Campus LAN and Wireless LAN Design Guide and the WAN Design Guide. All IP addressing is based off the Campus Wired LAN Design Guide. IP addresses used in this guide are examples; you should use addressing that is applicable to your architecture.

Cisco ISE has different personas, or modes, for which it can be configured: administration, policy service, and monitoring. For a standalone configuration where the appliance uses all personas, the maximum number of endpoints 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 appliances. In this example, there are six 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. The remaining nodes are for the pxGrid service and the SXP service. 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.

You can use shorthand references for the nodes. A node that runs the Administration persona is called a Policy Administration Node (PAN), a node that runs the Monitoring persona is called a Monitoring and Troubleshooting Node (MnT), and a node that runs the Policy Service persona is called a Policy Service Node (PSN).

Table 1  Cisco ISE node IP addresses and hostnames

<table>
<thead>
<tr>
<th>Device Persona</th>
<th>Shorthand</th>
<th>IP address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE primary Policy Administration Node and secondary Monitoring and Troubleshooting node</td>
<td>Primary PAN/Secondary MnT</td>
<td>10.4.48.41</td>
<td>ise-1.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE secondary Policy Administration Node and secondary Monitoring and Troubleshooting node</td>
<td>Secondary PAN/Primary MnT</td>
<td>10.4.48.42</td>
<td>ise-2.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE Policy Service Node</td>
<td>First PSN</td>
<td>10.4.48.43</td>
<td>ise-3.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE additional Policy Service Node</td>
<td>Additional PSN</td>
<td>10.4.48.44</td>
<td>ise-4.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE SXP Node</td>
<td>SXP PSN</td>
<td>10.4.48.40</td>
<td>ise-sxp.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE pxGrid Node</td>
<td>pxGrid</td>
<td>10.4.48.45</td>
<td>ise-pxgrid.cisco.local</td>
</tr>
</tbody>
</table>
Deploying ISE

1. Configure policy service node for SXP
2. Enable RADIUS profiling
3. Install Cisco ISE license
4. Configure network devices in Cisco ISE
5. Configure advanced TrustSec settings for Catalyst switches
6. Configure advanced TrustSec settings for NX-OS switches
7. Configure advanced TrustSec settings for Cisco ASA firewalls
8. Configure the RADIUS default device
9. Configure Cisco ISE to use Active Directory
10. Configuring ISE for authentication
11. Create security group tags
12. Configure TrustSec AAA servers
13. Configure security group access control lists
14. Create policy
15. Enable device authorization
16. Configure authorization profile
17. Configure authorization policy
18. Verify default policy is closed

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 should be used as a reference.

Reader Tip

Procedure 1  Configure policy service node for SXP

One of the PSNs installed is configured as an SXP node. In a distributed deployment, it is recommended that you deploy the SXP service on a PSN with no other services enabled.

**Step 1:** Using a browser, connect and log in to the PAN (example: https://ise-1.cisco.local).

**Step 2:** From the Administration menu, choose System, and then choose Deployment.

**Step 3:** In the Deployment Nodes list, choose the name of the node you will configure as the SXP PSN.

**Step 4:** Select Policy Service.

**Step 5:** In the Policy Service section, select Enable SXP Service, and then select the interface to use.

Step 6: Click Save.
**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.

---

**Procedure 2  Enable RADIUS profiling**

You can use Cisco ISE to profile endpoints in order to determine what types of devices are accessing the network using information contained in the RADIUS transactions. You can use this information to create specific policies for different endpoints. Although enabling profiling is not required in this deployment, it is useful to do so for better visibility into the endpoints accessing the network.

**Step 1:** Navigate to Administration > System > Deployment.

**Step 2:** In the Deployment Nodes list, choose one of the policy service nodes.

**Step 3:** On the General Setting tab, in the Policy Service section, select *Enable Profiling Service*.

**Step 4:** On the Profiling Configuration tab, select *RADIUS*.

**Step 5:** Click *Save*.

**Step 6:** For each additional PSN, repeat Step 1 through Step 5.
**Procedure 3**  **Install Cisco ISE license**

Cisco ISE comes with a 120-day demo license for both the Base and Advanced packages. To go beyond 120 days, you need to obtain a license from Cisco. In a distributed deployment, you need to install only the license on the primary administration node.

*Tech Tip*

When installing a Base license and an Advanced license, you must install the Base license first.

**Step 1:** Navigate to Administration > System > Licensing.

**Step 2:** In the License Files section, click Import License.

**Step 3:** Click Browse, locate your license file, and then click Import.

**Step 4:** If you have multiple licenses to install, repeat Step 2 and Step 3 for each.

**Procedure 4**  **Configure network devices in Cisco ISE**

Configure Cisco ISE to accept authentication requests from network devices. RADIUS requires a shared secret key to enable encrypted communications. Each network device that uses Cisco ISE for authentication need to have this key. You can configure each network device individually or group devices by location, by device type, or by using IP address ranges. The other option is to use the Default Device to configure the parameters for devices that aren’t specifically configured.

**Step 1:** Navigate to Administration > Network Resources > Network Devices.

**Step 2:** Click Add.
Step 3: Enter a name, description (optional), and IP address for the device.

Step 4: In the Device Profile list, choose Cisco.

Step 5: Select RADIUS Authentication Settings. The section expands.

Step 6: Enter the RADIUS Shared Secret.

Step 7: To better organize and identify devices, it’s desirable to use Device Groups to identify the type of device as well as its location.

Step 8: In the Device Type list, choose a device type. You can create a new device type by clicking on the gear icon in the upper right corner and selecting Create New Network Device Group.

Step 9: In the Parent list, choose the parent device group.

Step 10: Enter a name and (optionally) description, and then click Save.

Step 11: From the Device Type list, choose the newly created device type.
Step 12: In the Location list, choose a location. You can create a new location by clicking on the gear icon in the upper right corner and selecting Create New Network Device Group.

Step 13: In the Parent list, choose the parent device group.

Step 14: Enter a name and (optionally) description, and then click Save.

Step 15: From the Location list, choose the newly created location.

**Tech Tip**

You can also configure Network Device Groups by navigating to Administration > Network Resources > Network Device Groups. You can define all of the groups prior to adding the network devices.

With the exception of the wireless LAN controllers, when defining a network device for use in a TrustSec environment, you need to configure the Advanced TrustSec Settings section. This allows the network device to download the TrustSec environment data and policy and also to perform enforcement. The options vary depending on the network device, and they are covered below.

**Procedure 5** Configure advanced TrustSec settings for Catalyst switches

Step 1: Select Advanced TrustSec Settings. The section expands.

Step 2: In the Device Authentication Settings section, make sure Use Device ID for TrustSec Identification box is selected (to use the device name defined in the previous procedure), and then enter a password.

Step 3: In the TrustSec Notifications and Updates section, enter the frequency at which environment and policy updates will occur. The default values are 1 day.
Step 4: Select Other TrustSec devices to trust this device. Peer devices will not change the SGTs on packets arriving from this network device.

Step 5: If the device will be used to enforce policy, select Send configuration changes to this device, and then select CoA. This enables ISE to send policy changes to the network device.

Step 6: Click Submit.

**Procedure 6** Configure advanced TrustSec settings for NX-OS switches

Step 1: Select Advanced TrustSec Settings. The section expands.

Step 2: In the Device Authentication Settings section, make sure the Use Device ID for TrustSec Identification box is selected (to use the device name defined in the previous procedure), and then enter a password.

Step 3: In the TrustSec Notifications and Updates section, enter the frequency at which environment and policy updates will occur. The default values are 1 day.

Step 4: Select Other TrustSec devices to trust this device. Peer devices will not change the SGTs on packets arriving from this network device.

Step 5: If the device will be used to enforce policy, select Send configuration changes to this device, and then select CLI (SSH). Leave the Ssh Key field blank. This enables ISE to send policy changes to the network device.

Step 6: In the Device Configuration Deployment section, select Include this device when deploying Security Group Tag Mapping Updates.
Step 7: Enter the EXEC Mode Username, EXEC Mode Password, and Enable Mode Password. This allows ISE to access the network device.

Step 8: Click Submit.

**Procedure 7** Configure advanced TrustSec settings for Cisco ASA firewalls

Step 1: Select Advanced TrustSec Settings. The section expands.

Step 2: In the Device Authentication Settings section, make sure Use Device ID for TrustSec Identification box is selected (to use the device name defined in the previous procedure), and then enter a Password.

**Tech Tip**

Because Cisco ASA supports out-of-band protected access credentials (PAC) provisioning, the password is not used. However, in order to save the network device configuration, there must be a value in this box.
Step 3: In the TrustSec Notifications and Updates section, enter the frequency environment and policy updates will occur. The default values are 1 day.

Step 4: Select Other TrustSec devices to trust this device. Peer devices will not change the SGTs on packets arriving from this network device.

Step 5: In the Out Of Band (OOB) TrustSec PAC section, click Generate PAC.

Step 6: Enter an encryption key and the PAC time to live, and then click Generate PAC. You are prompted to save the file to your local machine.

![Generate PAC](image)

Step 7: Choose a location, and then click OK.

Step 8: Click Submit.

Step 9: Later in this guide, you will import this PAC into Cisco ASA.

Procedure 8 Configure the RADIUS default device

Step 1: Navigate to Administration > Network Resources > Network Devices.

Step 2: In the navigation panel on the left, click Default Device.

Step 3: In the Default Network Device Status list, choose Enable.
Step 4: Enter the RADIUS shared secret, and then click **Save**. The default network device configuration is now saved.

![Default Network Device Configuration](image)

**Procedure 9 Configure Cisco ISE to use Active Directory**

Cisco ISE uses the existing AD server as an external authentication server. First, you must configure the external authentication server.

**Step 1:** Navigate to **Administration > Identity Management > External Identity Sources**.

**Step 2:** In the left panel, click **Active Directory**, and then click **Add**.

**Step 3:** Enter a join point name and the Active Directory domain.

**Step 4:** Click **Submit**.

**Step 5:** In the message asking if you’d like to join all ISE nodes to the domain, click **Yes**.
Step 6: In the Join Domain window, enter an AD User Name and Password. If the organizational unit must be provided, select Specify Organizational Unit and enter it. Click OK.

![Join Domain](image)

Step 7: In the Join Operation Status window, click Close.

![Join Operation Status](image)

Next, you select the AD groups that Cisco ISE uses for authentication.

Step 8: Click on the Groups tab, click Add, and then click Select Groups from Directory.

Step 9: Search for the groups you wish to add. The domain box is already filled in. The default filter is a wildcard to list all groups. To get a list of all groups in your domain, click Retrieve Groups.

![Select Directory Groups](image)
Step 10: Select the groups you want to use for authentication, and then click OK. For example, for all users in the domain, select the group `<domain>/Users/Domain Users`. In this deployment, there are four groups that are assigned SGTs. They are Finance, HR, IT, and Research. Select those groups as well.

Step 11: Click Save.

Procedure 10 Configuring ISE for authentication

Now that ISE has a basic configuration, you configure an authentication policy for devices and users accessing the network.

Step 1: Navigate to Policy > Authentication. The Policy Type is Rule-Based.

There are already three preconfigured rules in place, MAB, Dot1X, and the default rule, which is the final, catch-all rule.

Step 2: For the Dot1X rule, click Edit. In the Use list, click the + symbol. The identity store used for this rule appears.

Step 3: In the Identity Source list, choose All_User_ID_Stores. This allows you to use both the internal database and the external Active Directory database for 802.1X authentication.
Procedure 11  Create security group tags

With authentication configured, you configure the security group tags (SGTs) used for authorization.

Step 1: Navigate to Work Centers > TrustSec > Settings, and then in the left navigation pane, click General TrustSec Settings.

Step 2: The default configuration of ISE is for the system to assign the SGT numbers. This example deployment uses manually assigned SGT numbers, which provides more flexibility and aids in troubleshooting.

Step 3: In the Security Group Tag Numbering section, select User Must Enter SGT Numbers Manually.

Step 4: Click Save.

Step 5: Navigate to Work Centers > TrustSec > Components, and then in the left navigation pane, click Security Groups.

Step 6: For convenience, there are already several security groups defined for some common classifications, such as Employees, Contractors, and Developers.

Step 7: Click Add. The New Security Group window opens.
Step 8: In this deployment, there are four departments: Finance, HR, IT, and Research. Each department has two security groups: one for users and one for servers. The security group names and tag values are listed in the table below:

<table>
<thead>
<tr>
<th>Security group name</th>
<th>Security group tag value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance_Servers</td>
<td>1000</td>
</tr>
<tr>
<td>Finance_Users</td>
<td>1001</td>
</tr>
<tr>
<td>HR_Servers</td>
<td>2000</td>
</tr>
<tr>
<td>HR_Users</td>
<td>2001</td>
</tr>
<tr>
<td>IT_Servers</td>
<td>3000</td>
</tr>
<tr>
<td>IT_Users</td>
<td>3001</td>
</tr>
<tr>
<td>Research_Servers</td>
<td>4000</td>
</tr>
<tr>
<td>Research_Users</td>
<td>4001</td>
</tr>
</tbody>
</table>

Step 9: Enter a Name for the security group, select an Icon, and (optionally) enter a Description and Tag Value.

Step 10: Click Submit.

Step 11: For each group in Table 2, repeat this procedure.
Procedure 12  Configure TrustSec AAA servers

In a multinode ISE deployment, each PSN needs to be added as a TrustSec AAA server.

Step 1: Navigate to Work Centers > TrustSec > Components, and then in the left navigation pane, click Trustsec AAA Servers.

Step 2: Click Add.

Step 3: Enter the name of the PSN, (optionally) a description, and the IP address. The default value of 1812 for the port is already entered.

Step 4: For every PSN in the deployment, repeat this procedure. Also, if the primary PAN is already configured as an AAA server, now you can delete it.

Procedure 13  Configure security group access control lists

Step 1: With security groups defined, you next create Security Group Access Control Lists (SGACLs) that are used to define the policy enforced in the deployment. The policy enforced is that intra-departmental traffic is permitted but inter-departmental traffic is denied. For example, users in HR are able to communicate with each other and with the HR servers. In addition, HR servers can communicate with each other. This policy is just an example and you should create a policy that meets your organization’s needs.

Step 2: Navigate to Work Centers > TrustSec > Components, and then in the left navigation pane, click Security Group ACLs.

Step 3: Click Add. The New Security Group ACLs window opens.
Step 4: The following table lists the SGACLs to be configured:

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Version</th>
<th>Security Group ACL Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance_ACL</td>
<td>IPv4</td>
<td>permit ip log</td>
</tr>
<tr>
<td>HR_ACL</td>
<td>IPv4</td>
<td>permit ip log</td>
</tr>
<tr>
<td>IT_ACL</td>
<td>IPv4</td>
<td>permit ip log</td>
</tr>
<tr>
<td>Research_ACL</td>
<td>IPv4</td>
<td>permit ip log</td>
</tr>
<tr>
<td>Deny_All</td>
<td>IPv4</td>
<td>deny ip log</td>
</tr>
</tbody>
</table>

Step 5: Enter the name and (optionally) description, and under **IP Version**, select **IPv4**.

Step 6: In the **Security Group ACL content** field, enter in the ACL to be used.

Step 7: Click Submit.

Step 8: For each ACL in Table 3, repeat this procedure.
Procedure 14  Create policy

With the SGTs and SGACLs defined, you now create the policy by assigning the SGACLs to source and destination group pairs. In this deployment, the policy enforced is that intra-departmental traffic is permitted but inter-departmental traffic is denied. For example, users in HR are able to communicate with each other and with the HR servers. In addition, HR Servers can communicate with each other. The policy is defined in a matrix where the source is listed on the left and the destination is listed on the top. At the intersection for a given pair, the SGACL listed is the enforced policy.

Table 4  TrustSec egress policy matrix

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Finance_Users</th>
<th>Finance_Servers</th>
<th>HR_Servers</th>
<th>HR_Users</th>
<th>IT_Servers</th>
<th>IT_Users</th>
<th>Research_Servers</th>
<th>Research_Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance_Servers</td>
<td>Finance_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
</tr>
<tr>
<td>Finance_Users</td>
<td>Finance_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
</tr>
<tr>
<td>HR_Servers</td>
<td>HR_ACL</td>
<td>Deny_All</td>
<td>HR_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
</tr>
<tr>
<td>HR_Users</td>
<td>HR_ACL</td>
<td>Deny_All</td>
<td>HR_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
</tr>
<tr>
<td>IT_Servers</td>
<td>IT_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>IT_ACL</td>
<td>IT_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
</tr>
<tr>
<td>IT_Users</td>
<td>IT_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>IT_ACL</td>
<td>IT_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
</tr>
<tr>
<td>Research_Servers</td>
<td>Research_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Research_ACL</td>
<td>Research_ACL</td>
<td>Deny_All</td>
<td>Research_ACL</td>
</tr>
<tr>
<td>Research_Users</td>
<td>Research_ACL</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Deny_All</td>
<td>Research_ACL</td>
<td>Research_ACL</td>
<td>Deny_All</td>
<td>Research_ACL</td>
</tr>
</tbody>
</table>

Step 1: Navigate to Work Centers > TrustSec > Policy, and then in the left navigation pane, in the Egress Policy section, click Matrix.

Step 2: Double-click in the intersection of the source and destination groups to edit the policy.

Step 3: Verify that the Status is Enabled and optionally provide a description.

Step 4: On the Assigned Security Group ACLs section, in the list, choose the previously defined SGACL.
Step 5: Click Save.

![Edit Permissions...](image)

Step 6: For every source and destination group pair in Table 4, repeat this procedure.

**Procedure 15  Enable device authorization**

Now that policy has been created, you need to enable authorization for the devices where policy is to be enforced. In this deployment, enforcement is going to occur at the Nexus 7000s in the data center.

**Step 1:** Navigate to Work Centers > TrustSec > Policy, and then in the left navigation pane, click Network Device Authorization.

**Step 2:** On the right of the default rule, click the black triangle, and then select Insert new row above.

**Step 3:** Enter a name for the rule, and then click the + symbol next to Condition(s).
Step 4: Click Create New Condition (Advance Option).

Step 5: You need to identify the switches defined previously as a network device. In this deployment, they were added to the DC Switch group, and this is what this rule uses.

Step 6: In the Expression list, choose Device Type.

Step 7: In the second list, make sure Equals is chosen.

Step 8: In the third list, choose All Device Types#DC Switch.

Step 9: In the Security Group list, choose TrustSec_Devices.

Step 10: Click Done, and then click Save.

Procedure 16 Configure authorization profile

This deployment is using 802.1X in what is called low-impact mode. In low-impact mode, the wired port is configured with a pre-authentication access list that limits what the endpoint connected to the port can access in an unauthenticated state. Once the endpoint passes authentication, a downloadable access list is passed from ISE to the switch. In this deployment, the access list simply permits all traffic, but you can tailor this to suit the needs of your deployment. For wireless endpoints, the access list is configured on the WLAN controller and the authorization policy instructs the WLC to use that ACL after authentication.

Step 1: Navigate to Policy > Policy Elements > Results, and then in the left navigation pane, expand the Authorization section and click Authorization Profiles.

Step 2: Click Add.
Step 3: Name the profile and (optionally) description, and then in the Access Type list, choose ACCESS_ACCEPT.

![Authorization Profile](image)

Step 4: In the Common Tasks section, select DACL Name, and then in the list, choose PERMIT_ALL_TRAFFIC.

![Common Tasks](image)

Step 5: In the Common Tasks section, select Airespace ACL Name, and then in the box, type a name for the ACL you will configure on the WLC. This is covered in a later section of this guide.

![Common Tasks](image)

Step 6: Click Submit.

Step 7: For each group for which you have defined policy, repeat this procedure. In this deployment, the groups are Finance, HR, IT, and Research.
Procedure 17  Configure authorization policy

All of the elements of the authorization policy are defined, and now you configure the authorization policy that assigns SGTs to users when they authenticate to the network.

Step 1: Navigate to Policy > Authorization.

Step 2: For the existing Profiled Non Cisco IP Phones rule, on the right, click the black triangle symbol, and then select Insert New Rule Below. A new rule named Standard Rule 1 is created.

Step 3: Rename the newly created rule to match one of the groups for which you will define policy. (Example: HR Users)

Step 4: In the Condition(s) list, choose the + symbol, and then click Create New Condition (Advance Option).

Step 5: In the next column, choose Equals.

Step 6: In the final column, choose cisco.local/Users/HR.

Step 7: In the Permissions column, next to AuthZ Profile(s), click the + symbol.

Step 8: In the Select an item list, choose Standard, and then select the authorization profile that was created in Procedure 16, “Configure authorization profile”. (Example: HR)

Step 9: Click the + symbol to add another entry.

Step 10: In the Select an item list, choose Security Group, and then select the SGT that was created in Procedure 11, “Create security group tags.” (Example: HR_Users)

Step 11: Click Done, and then click Save.

Step 12: For each group that requires an authorization policy, repeat this procedure. In this deployment the groups are Finance, HR, IT, and Research.
Procedure 18  Verify default policy is closed

The default rule at the end of the authorization policy specifies the action to take if an incoming authorization request doesn’t match one of the specific rules defined. Since you have created rules for users, you want to make sure the default action is to deny access if the request didn’t match any other rules.

Step 1: Navigate to Policy > Authorization.

Step 2: In the row for the default rule, click Edit.

Step 3: If the action listed is in the Conditions column is PermitAccess, then click the + symbol. A selection box opens.

Step 4: In the list, choose Standard, and then choose DenyAccess.

Step 5: Click Done, and then click Save. The updated authorization policy appears.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit +</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enabling Wired Authentication

1. Enable RADIUS in the wired access layer
2. Enable identity on the wired access ports
3. Disable port security timers

The policy for network access is now defined and the next step is to enable 802.1X in the wired access layer to authenticate and authorize the users.

Procedure 1  Enable RADIUS in the wired access layer

Step 1: Identify switches in the access layer, connect to the console of each access switch, and configure each with the following RADIUS and AAA global configuration commands.

```
radius server ise-3
address ipv4 10.4.48.43 auth-port 1812 acct-port 1813
key [radius key]
radius server ise-4
address ipv4 10.4.48.44 auth-port 1812 acct-port 1813
```
key [radius key]

aaa group server radius ISE_GROUP
server name ise-3
server name ise-4

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

radius-server vsa send accounting
radius-server vsa send authentication
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include

**Tech Tip**

For consistency among this guide and other CVD guides, we have standardized on these well-known TCP ports for RADIUS authentication and accounting: 1812 and 1813. Cisco ISE supports both the older IOS default of 1645/1646 ports and the newer standardized 1812/1813 ports.

---

**Procedure 2**  
Enable identity on the wired access ports

**Step 1:** Connect to the console of each access switch, and configure each with the following identify global configuration commands. The device-sensor command is not available on all switches.

- authentication mac-move permit
- dot1x system-auth-control
- device-sensor accounting

**Tech Tip**

The device sensor functionality is only available for switches that use specific software versions and feature sets. If available, it should be enabled to add additional profiling visibility by gathering data gleaned from traffic coming from endpoints.
Step 2: Enable device tracking. Device tracking populates the dynamically learned IP address into the downloadable ACL.

```bash
ip device tracking
```

Step 3: You create an access list to limit traffic that is permitted on a port before it is authenticated, to allow only the traffic that is required for the port to go through the authentication process. Permitted traffic typically includes DHCP, DNS, TFTP for Preboot Execution Environment, and access to the AD domain controller. For troubleshooting, you also allow ICMP echo and echo-reply traffic. The list denies all other traffic.

```bash
ip access-list extended PreAuth
    remark Pre-authorization ACL for 802.1X
    permit ip any host 10.4.48.10
    permit udp any eq bootpc any eq bootps
    permit udp any any eq domain
    permit udp any any eq tftp
    permit icmp any any echo
    permit icmp any any echo-reply
    deny ip any any
```

Step 4: Authorization requires the use of RADIUS Change of Authorization (CoA) in order to change the state of the port after authentication. This is not enabled by default, so you enable it.

```bash
aaa server radius dynamic-author
    client 10.4.48.43 server-key [radius key]
    client 10.4.48.44 server-key [radius key]
    auth-type any
```

To make configuration easier when the same configuration is applied to multiple interfaces on the switch, use the `interface range` command. This command allows you to issue a command once and have it apply to many interfaces at the same time. Because most of the interfaces in the access layer are configured identically, it can save a lot of time. For example, the following command allows you to enter commands on all 24 interfaces (Gig 0/1 to Gig 0/24) simultaneously.

```bash
interface range GigabitEthernet 0/1-24
```
Step 5: Connect to the console of each access switch, and configure all host access ports on each. These commands should not be configured on infrastructure-facing ports, such as uplinks.

```
interface range [interface type] [port number]-[port number]
  ip access-group PreAuth in
  authentication host-mode multi-domain
  authentication open
  authentication order dot1x mab
  authentication port-control auto
  mab
  dot1x pae authenticator
```

**Tech Tip**

On the Catalyst 3650/3850, there is a caveat where TrustSec inline tagging is incompatible with IP Source Guard (ip verify source). If you plan on using inline tagging, you need to disable IP Source Guard on the access port. This will be resolved in a future software release.

---

**Procedure 3 Disable port security timers**

The [Campus Wired LAN Technology Design Guide](#) incorporates the use of port security to provide a level of security and prevent rogue devices from being connected. However, 802.1X also provides similar functionality and there can be conflicts when both are enabled on a port at the same time. As an example, both port security and 802.1X each have their own set of inactivity timers. Enabling both simultaneously causes 802.1X to re-authenticate every time the port security timeout is reached. To avoid this issue and other potential conflicts, disable port security.

**Step 1:** Remove the port security configuration.

```
interface range [interface type] [port number]-[port number]
  no switchport port-security aging time
  no switchport port-security aging type
  no switchport port-security violation
  no switchport port-security
```
Enabling Wireless Authentication

1. Add ISE as RADIUS authentication server
2. Add Cisco ISE as RADIUS accounting server
3. Enable client profiling
4. Configure WLC for authorization

To authenticate wireless clients, you need to configure the WLC to use the new Cisco ISE servers as RADIUS servers for authentication and accounting. The existing entry is disabled so that if there are any issues after moving to Cisco ISE, you can quickly restore the original configuration. Additionally, you configure the WLCs for device profiling so that profiling information can be obtained from the DHCP and HTTP requests from these clients and sent to the Cisco ISE.

Procedure 1  Add ISE as RADIUS authentication server

Perform this procedure for every WLAN controller used for employee access.

Step 1: Use a web browser to connect and log in to the WLC console. (Example: https://wlc1.cisco.local)

Step 2: On the top menu bar, click Security.

Step 3: In the left pane, under the AAA > RADIUS section, click Authentication.

Step 4: Do not make changes to any preexisting RADIUS servers yet. Click New. You can now configure a new RADIUS Authentication server.

Step 5: In the Server IP Address box, enter your primary ISE policy service node IP address, 10.4.48.43.

Step 6: In the Shared Secret box, enter your RADIUS shared secret, and then in the Confirm Shared Secret box, re-enter it.

Step 7: In the Support for CoA list, choose Enabled.
Step 8: Next to Management, clear Enable, and then click Apply.

Step 9: Repeat Step 4 through Step 8 in order to add the additional ISE policy service node 10.4.48.44 to the WLC configuration.

If a RADIUS server was previously configured on the WLC, you disable the preexisting RADIUS server. By disabling the server instead of deleting it, you can easily switch back, if needed.

Step 10: If you have a preexisting RADIUS server, on the RADIUS Authentication Servers screen under Server Index, click the number of the preexisting RADIUS server. On the Edit screen, change Server Status to Disabled, and then click Apply.

You are returned to the RADIUS Authentication Servers screen, where you can see the Admin Status for the preexisting server is Disabled.

Step 11: For every remaining WLC in your network, repeat this procedure.
Procedure 2  Add Cisco ISE as RADIUS accounting server

Step 1: On the menu bar, click Security.

Step 2: In the left pane, under the RADIUS section, click Accounting.

Step 3: Do not make changes to any preexisting RADIUS servers yet. Click New. You can now configure a new RADIUS accounting server.

Step 4: In the Server IP Address box, enter your primary ISE policy service node IP address, **10.4.48.43**.

Step 5: In the Shared Secret box, enter your RADIUS shared secret, and then in the Confirm Shared Secret box, re-enter it.

Step 6: Repeat Step 3 through Step 5 and add the additional ISE policy service node **10.4.48.44** to the WLC configuration.
Step 7: If you have a preexisting RADIUS server, on the RADIUS Accounting Servers screen under Server Index, click the number of the preexisting RADIUS server. On the Edit screen, change Server Status to Disabled, and then click Apply.

You are returned to the RADIUS Accounting Servers screen, where you can see the Admin Status for the preexisting server is Disabled.

---

**Procedure 3**  Enable client profiling

You need to enable client profiling on the WLC in order to send DHCP and HTTP information to the engine for endpoint profiling.

Step 1: On the WLC, navigate to WLANs, and then select the WLAN ID underlined number for an SSID you wish to monitor.

Step 2: On the Advanced tab, in the Radius Client Profiling section, select DHCP Profiling.

Step 3: Select HTTP Profiling, click Apply, and then click OK in order to acknowledge there may be a WLAN connectivity disruption.

Step 4: At the top right, click Save Configuration, and then click OK to confirm.
Procedure 4  Configure WLC for authorization

The WLC does not support downloadable ACLs like the switches. Instead, you define the ACL on the WLC, and when clients connect to the WLC and authenticate, in the campus and at remote sites with a local controller, Cisco ISE passes a RADIUS attribute requesting that the ACL be applied for this client.

Step 1: On the WLC, navigate to Security.

Step 2: In the left pane, in Access Control Lists, choose Access Control Lists, and then click New.

Step 3: Name the access list, and then click Apply.

Step 4: Click the name in the list. This allows you to edit the newly created access list.

Step 5: Click Add New Rule.

Step 6: Create a new access list rule based on your security policy, and then click Apply. This example deployment allows full access to authenticated users.

Tech Tip

The access list needs to have entries for the traffic in both directions, so make sure you have pairs of access list rules for both inbound and outbound traffic. Also, there is an implicit “deny all” rule at the end of the access list, so any traffic not explicitly permitted is denied.

Step 7: For each access list that you defined in the authorization profiles in Cisco ISE, repeat Step 2 through Step 6.

Next, you enable WLC to allow Cisco ISE to use RADIUS to override the current settings, so that the access list can be applied to the WLAN.

Step 8: On the WLC menu bar, click WLANs.

Step 9: Click the WLAN ID of the wireless network that the wireless personal devices are accessing.
Step 10: Click Advanced, and then select Allow AAA Override.

Step 11: Click Apply, and then click Save Configuration.

Step 12: The infrastructure is now configured to assign tags to users when they login to the network. Below shows the authentication session details for a logged in wired user on a Catalyst switch and a logged in wireless user on a WLC. You can see the assigned SGT and dACL associated with these users.

Step 13: Example on a Catalyst Switch:

```
AD5-3650# show authentication sessions interface gigabitEthernet 1/0/2 details
Interface:  GigabitEthernet1/0/2
IIF-ID:  0x1076B4000000260
MAC Address:  0050.5689.5190
IPv6 Address:  Unknown
IPv4 Address:  10.4.112.182
User-Name:  CISCO\hr_user
Status:  Authorized
Domain:  DATA
Oper host mode:  multi-auth
Oper control dir:  both
Session timeout:  N/A
Restart timeout:  N/A
Session Uptime:  235050s
Common Session ID:  0A047F050000117012E1599E
Acct Session ID:  0x00001702
Handle:  0xCF00019C
Current Policy:  POLICY_Gi1/0/2
Local Policies:  
    Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
    Server Policies:
        ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-56161e32
        SGT Value:  2001
Method status list:  
    Method  State
    dot1x  Authc Success
```
Step 14: Example on a WLC:

Assigning SGTs to Servers

1. Enable TrustSec on NX-OS switches
2. Configure IP-to-SGT binding on the NX-OS switch
3. Configure IP-to-SGT binding in ISE

Now that the users are assigned SGTs, you need to assign SGTs to the servers in the data center. Depending on the deployment, you can do this on the Nexus 7000s in the data center for physical servers or on a Nexus 1000v switch in a virtualized environment. For the physical servers, either you can define the SGT directly on the switch or you can use ISE to assign it.

Procedure 1: Enable TrustSec on NX-OS switches

Step 1: Connect to the console of the Nexus 7000 or Nexus 1000v in the data center, and then enable TrustSec.

```
feature dot1x
feature cts
```

Step 2: Enable TrustSec device authentication. The device-id and password you use are the ones defined in Procedure 6, “Configure advanced TrustSec settings for NX-OS switches”.

```
cts device-id DC-N7004-1 password [password]
```
Step 3: Define the RADIUS servers and AAA parameters.

radius-server host 10.4.48.43 key [RADIUS key] pac authentication accounting
radius-server host 10.4.48.44 key [RADIUS key] pac authentication accounting
aaa group server radius ISE_Group
    server 10.4.48.43
    server 10.4.48.44
    use-vrf management
aaa authorization cts default group ISE_Group
aaa accounting default group ISE_Group

Procedure 2 Configure IP-to-SGT binding on the NX-OS switch

Step 1: Connect to the console of the Nexus 7000 or Nexus 1000v in the data center, and then create an IP-to-SGT binding.

    cts role-based sgt-map [IP address of server] [SGT]

Step 2: For every server you will assign an SGT, repeat this procedure.

Procedure 3 Configure IP-to-SGT binding in ISE

Step 1: Connect and login to the PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to Work Centers > TrustSec > Policy. In the left navigation pane, expand Security Group Mappings, and then click Hosts.

Step 3: Click Add.

Step 4: Select IP address, and then enter the address of the server.

Step 5: Select Security Group Tag, and then select the SGT from the list.

Step 6: Select Network Device Group.

Step 7: In the drop-down list, click the arrow next to All Device Types, and then select the group to deploy the binding. In this deployment, the group is DC Switch.
Step 8: Click Submit.

Step 9: For every server you will assign an SGT, repeat this procedure.
Configuring SGT Propagation

1. Configure SXP on IOS devices
2. Configure SXP on WLCs
3. Configure SXP on ISE
4. Configure SXP on Cisco ASA
5. Configure SXP in NX-OS
6. Configure inline tagging in IOS switches
7. Configure inline tagging in NX-OS switches
8. Configure inline tagging on the Nexus 1000v with port profiles
9. Enable SXP on ISR
10. Enable inline tagging on the ISR
11. Enable inline tagging over DMVPN
12. Enable inline tagging over GET VPN

Now that tags are assigned to the users and servers, you need to propagate them to devices on the network. As discussed earlier in this guide, there are two methods of propagation. The first is SXP, and the second is via inline tagging in the data plane.

**Figure 11  Propagation using SXP**

SXP is a control plane protocol that propagates the IP-to-SGT mapping database from network authentication points such as access layer switches to upstream network devices. SXP is a TCP-based peering protocol. You can use SXP to propagate tags in an environment where all devices do not support inline tagging. It operates based on a peering relationship between two devices. One device is the speaker and sends IP-to-SGT bindings to the other peer. The second device is the listener and it receives the bindings from the speaker. A single device can have multiple peers and be both a speaker and a listener. A typical deployment has the access switch or WLC peer with a distribution switch, and then the distribution switch peers with the DC core to provide hierarchy.
Inline tagging occurs in the data plane, and the tag is embedded in the Cisco metadata in the Layer 2 header and carried throughout the network. This requires that all infrastructure along the path must support inline tagging and the configuration is placed on the interfaces connecting the devices.

**Figure 12 Propagation using inline tagging**

![Diagram showing propagation using inline tagging](image)

**TrustSec in the Campus**

**Procedure 1 Configure SXP on IOS devices**

**Step 1:** Connect to the console of the switch and configure SXP. The role of the device is either speaker or listener, depending on if the device is sending or receiving IP-to-SGT bindings.

```
cts sxp enable
cts sxp default source-ip [IP address of device]
cts sxp default password [password]
cts sxp connection peer [IP address of peer device] password default mode local [speaker|listener]
```

**Tech Tip**

The source IP address is typically the management IP address of the device or a loopback address.

An example configuration from a distribution switch that is a speaker to the DC switch and a listener to two access switches.

```
cts sxp enable
cts sxp default source-ip 10.4.15.254
```
cts sxp default password [password]
cts sxp connection peer 10.4.63.2 password default mode local speaker
cts sxp connection peer 10.4.15.5 password default mode local listener
cts sxp connection peer 10.4.15.6 password default mode local listener

Step 2: Verify the SXP connection.

D1-6807-VSS# show cts sxp connection
SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: 10.4.15.254
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running

----------------------------------------------
Peer IP : 10.4.15.5
Source IP : 10.4.15.254
Conn status : On
Conn version : 4
Conn capability : IPv4-IPv6-Subnet
Conn hold time : 120 seconds
Local mode : SXP Listener
Connection inst# : 9
TCP conn fd : 3
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 30:19:50:34 (dd:hr:mm:sec)

----------------------------------------------
Peer IP : 10.4.15.6
Source IP : 10.4.15.254
Conn status : On
Conn version : 4
Conn capability : IPv4-IPv6-Subnet
Conn hold time : 120 seconds
Local mode : SXP Listener
Connection inst# : 9
TCP conn fd      : 2
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 9:16:54:20 (dd:hr:mm:sec)

----------------------------------------------
Peer IP          : 10.4.63.3
Source IP        : 10.4.15.254
Conn status      : Off
Conn version     : 4
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: none
Duration since last state change: 0:00:01:57 (dd:hr:mm:sec)

Total num of SXP Connections = 3

Step 3: For each SXP device you add, repeat this procedure.

Procedure 2 Configure SXP on WLCs

Step 1: Use a web browser to connect and login to the WLC console (example: https://wlc1.cisco.local).

Step 2: Navigate to Security > TrustSec SXP.

Step 3: In the SXP State list, choose Enabled.

Step 4: Enter a default password.

Step 5: Click New.

Step 6: Enter the peer IP address for the peer device, and then click Apply.
Step 7: On the SXP Configuration screen, click **Apply**, and then click **Save Configuration**.

![SXP Configuration Screen](image)

Step 8: For each SXP device you will add, repeat this procedure.

**Procedure 3 Configure SXP on ISE**

A new feature in ISE 2.0 is the ability to run SXP on a PSN. This allows ISE to send and receive IP-to-SGT bindings. It also allows ISE to create IP to SGT bindings based on RADIUS sessions. An access device that then does 802.1X authentication or MAB using ISE but does not support TrustSec is able to participate in a TrustSec environment using this method. In the User-to-DC scenario with enforcement being done on the DC switches, ISE propagates these RADIUS session bindings to DC switches using SXP, without the need to configure any propagation method on the access switch.

**Step 1:** Using a browser, connect and login to the PAN (example: https://ise-1.cisco.local).

**Step 2:** Navigate to **Work Centers > TrustSec > Settings**, and in the left navigation pane, click **SXP Settings**.

**Step 3:** To place RADIUS mappings into the IP-SGT binding table, select **Add radius mappings into SXP IP SGT mapping table**.

**Step 4:** Enter the global password to be used for SXP connections.
Step 5: Click Save.

![Image of TrustSec settings in Identity Services Engine]

Step 6: You are prompted to restart the SXP service. Click Yes.

Step 7: Navigate to Work Centers > TrustSec > SXP, and in the left navigation pane, click SXP Devices.

Step 8: Click Add.

Step 9: Enter a name for the SXP device and the IP address.

Step 10: In the Peer Role list, choose the appropriate SXP role for this device. For example, the DC switches are listeners and the distribution switches are speakers.

Step 11: Click in the Connected PSNs box, and then select the SXP PSN configured in Procedure 1, “Configure policy service node for SXP.”

Step 12: In the Status list, choose Enabled.

Step 13: In the Password Type list, choose DEFAULT.
Step 14: In the Version list, choose V4.

**Tech Tip**

SXP negotiates the version to use between devices and selects the highest version available. Selecting SXP V4 ensures that the device negotiates the highest version it supports.

Step 15: Click Save.
Step 16: For each SXP device you will add, repeat this procedure.

Procedure 4 Configure SXP on Cisco ASA

Step 1: In a browser, navigate to the Cisco ASA management console (example: https://DC-ASA5585X.cisco.local), and then click Run ASDM.

Step 2: If you are using virtual contexts on your firewall, in the Device List, choose the context.

Step 3: Navigate to Configuration > Firewall > Identity by TrustSec.

Step 4: Select Enable SGT Exchange Protocol (SXP).

Step 5: In the Default Source box, enter the IP address of the interface of the Cisco ASA appliance used for management.

Step 6: Enter a password, and then confirm it.

Step 7: In the Server Group Setup section, click Manage.

Step 8: In the Configure AAA Server Group window, click Add.

Step 9: In the AAA Server Group box, enter a group name. (Example: ISE_Group)
Step 10: For Accounting Mode, select **Simultaneous**, and then click **OK**.

Step 11: In the Servers in the Selected Group section, click **Add**.

Step 12: In the **Interface Name** list, choose the firewall interface **mgmt**.

Step 13: In the **Server Name or IP Address** box, enter **ise-3.cisco.local**.

Step 14: In the RADIUS Parameters section, in **Server Authentication Port**, replace 1645 with 1812.

Step 15: In **Server Accounting Port**, replace 1646 with 1813.

Step 16: Enter the **Server Secret Key**.
Step 17: Accept the defaults for the remaining parameters, and then click **OK**.

![Add AAA Server](image)

Step 18: For the remaining PSNs in the deployment, repeat Step 11 through Step 17.

Step 19: Click **OK**. The Configure AAA Server Groups window closes.

Step 20: Click **Import PAC**.

Step 21: Click **Browse**.

Step 22: Locate the PAC file you saved to your machine in Procedure 7, “Configure Advanced TrustSec Settings for Cisco ASA Firewalls.”

Step 23: Enter the PAC password, and then confirm it.
Step 24: Click Import.

Step 25: When the import is complete, acknowledge the “PAC Imported Successfully” message. Now you add SXP peers to Cisco ASA.

Step 26: Click Add.

Step 27: Enter the IP address of the peer.

Step 28: In the Password list, choose Default.

Step 29: In the Mode list, choose Local.

Step 30: In the Role list, choose Listener, and then click OK.

Step 31: For each peer you need to add, repeat Step 26 through Step 30.
Step 32: Click Apply.

Procedure 5 Configure SXP in NX-OS

Step 1: Connect to the console of the switch and configure SXP. The role of the device is either speaker or listener, depending on if the device is sending or receiving IP-to-SGT bindings.

```bash
cts sxp enable
cts sxp default password <password>
cts sxp default source-ip [IP address of device]
cts sxp connection peer [IP address of peer device] password default mode local [speaker|listener] vrf [VRF for this connection]
```

**Tech Tip**

In a User-to-DC deployment, the Nexus 7000 is typically just an SXP listener and learns all of the IP-to-SGT bindings from other devices on the network. The Nexus 1000v supports speaker mode only.

Step 2: If you have a Nexus 1000v, configure IP device tracking.
Below is an example configuration from a data center switch that is a listener to two distribution switches and a speaker to two ASA firewalls. Note that the firewalls are using different source interfaces.

```
ccts sxp enable
cts sxp default source-ip 10.4.63.2
cts sxp default password [password]
cts sxp connection peer 10.4.15.254 password default mode local listener vrf default
cts sxp connection peer 10.4.175.254 password default mode local listener vrf default
cts sxp connection peer 10.4.51.20 source 10.4.51.19 password default mode local speaker vrf default
cts sxp connection peer 10.4.51.36 source 10.4.51.35 password default mode speaker vrf default
```

### Step 3: Verify the SXP connection.

```
DC-N7004-1# show cts sxp connection

<table>
<thead>
<tr>
<th>PEER_IP_ADDR</th>
<th>VRF</th>
<th>PEER_SXP_MODE</th>
<th>SELF_SXP_MODE</th>
<th>CONNECTION STATE</th>
<th>VERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.4.15.254</td>
<td>default</td>
<td>speaker</td>
<td>listener</td>
<td>connected</td>
<td>3</td>
</tr>
<tr>
<td>10.4.48.40</td>
<td>default</td>
<td>speaker</td>
<td>listener</td>
<td>connected</td>
<td>3</td>
</tr>
<tr>
<td>10.4.51.20</td>
<td>default</td>
<td>listener</td>
<td>speaker</td>
<td>connected</td>
<td>1</td>
</tr>
<tr>
<td>10.4.51.36</td>
<td>default</td>
<td>listener</td>
<td>speaker</td>
<td>connected</td>
<td>1</td>
</tr>
<tr>
<td>10.4.175.254</td>
<td>default</td>
<td>speaker</td>
<td>listener</td>
<td>connected</td>
<td>3</td>
</tr>
</tbody>
</table>
```

### Step 4: For each SXP device you will add, repeat this procedure.

#### Tech Tip

For MD5 authentication, SXP makes use of TCP option field. If you have SXP peers that establish a connection through a firewall, you need to make sure that the firewall does not strip the TCP options and to also not perform TCP sequence number randomization. The following commands allow SXP peers to establish a connection through a Cisco ASA firewall.

```
access-list SXP-MD5-ACL extended permit tcp host <SXP_Peer_A> host <SXP_Peer_B> eq 64999
access-list SXP-MD5-ACL extended permit tcp host <SXP_Peer_B> host <SXP_Peer_A> eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
tcp-options range 19 19 allow
```
class-map **SXP-MD5-CLASSMAP**
match access-list **SXP-MD5-ACL**

policy-map global_policy
class **SXP-MD5-CLASSMAP**
set connection random-sequence-number disable
set connection advanced-options **SXP-MD5-OPTION-ALLOW**
set connection advanced-options tcp-state-bypass
service-policy global_policy global

---

**Procedure 6** Configure inline tagging in IOS switches

**Step 1:** Connect to the console of the switch and configure inline tagging.

```plaintext
interface [interface type] [port number]
  shutdown
  no cts role-based enforcement
  cts manual
  policy static sgt 2 trusted
  no shutdown
```

**Tech Tip**

To ensure the new TrustSec policy takes effect, you need to reset the interface by shutting it down and then re-enabling it. To use TrustSec in the most scalable manner, we recommend turning off enforcement on links between TrustSec-capable devices in order to ensure that filtering is done on egress from the TrustSec environment.

SGT 2 is the tag reserved for TrustSec Devices, and the keyword **trusted** tells this switch to trust tags coming into this interface and not overwrite an existing tag.

**Tech Tip**

If you are configuring inline tagging on a port-channel interface, you need to first remove the interfaces from the port-channel and then apply the TrustSec configuration to each physical interface.

**Step 2:** Verify the inline configuration. You’ll see that TrustSec is in manual mode and that authorization was successful, using an SGT of 2.

```plaintext
show cts interface [interface type] [port number]
```
Example:

```
C1-6807-VSS#show cts interface TenGigabitEthernet 1/5/1
```

Global Dot1x feature is Disabled

Interface TenGigabitEthernet1/5/1:

- **CTS is enabled, mode:** MANUAL
- **IFC state:** OPEN
- **Interface Active for:** 1w0d
- **Authentication Status:** NOT APPLICABLE
  - **Peer identity:** "unknown"
  - **Peer’s advertised capabilities:** ""
- **Authorization Status:** SUCCEEDED
- **Peer SGT:** 2:TrustSec_Devices
- **Peer SGT assignment:** Trusted
- **SAP Status:** NOT APPLICABLE
- **Propagate SGT:** Enabled
- **Cache Info:**
  - **Expiration:** N/A
  - **Cache applied to link:** NONE

**Step 3:** For each interface you wish to configure for inline tagging, repeat this procedure.

**Procedure 7**  
**Configure inline tagging in NX-OS switches**

**Step 1:** Connect to the console of the switch and configure inline tagging.

```
interface [interface type] [port number]
shutdown
crs manual
  policy static sgt 2 trusted
no shutdown
```

**Tech Tip**

To ensure the new TrustSec policy takes effect, you need to reset the interface by shutting it down and then re-enabling it.

SGT 2 is the tag reserved for TrustSec Devices and the keyword trusted tells this switch to trust tags coming into this interface and not overwrite an existing tag.
**Tech Tip**

If you are configuring inline tagging on a port-channel interface, you can configure it directly on the port-channel interface, and the configuration is copied to the physical interface.

**Step 2:** Verify the inline configuration. You’ll see that TrustSec is in manual mode and that authorization was successful, using an SGT of 2.

```
show cts interface [interface type] [port number]
```

As an example:

```
DC-N7004-1# show cts interface Ethernet 3/41
CTS Information for Interface Ethernet3/41:
  CTS is enabled, mode: CTS_MODE_MANUAL
  IFC state: CTS_IFC_ST_CTS_OPEN_STATE
  Authentication Status: CTS_AUTHC_SKIPPED_CONFIG
    Peer Identity:
      Peer is: Unknown in manual mode
      802.1X role: CTS_ROLE_UNKNOWN
    Last Re-Authentication:
      Authorization Status: CTS_AUTHZ_SKIPPED_CONFIG
      PEER SGT: 2(TrustSec_Devices)
      Peer SGT assignment: Trusted
  SAP Status: CTS_SAP_SKIPPED_CONFIG
  Version:
    Configured pairwise ciphers:
    Replay protection:
    Replay protection mode:
    Selected cipher:
    Propagate SGT: Enabled
```

**Step 3:** For each interface you wish to configure for inline tagging, repeat this procedure.
**Procedure 8** Configure inline tagging on the Nexus 1000v with port profiles

To configure the switchport on the Nexus 1000v to assign an SGT, you use a port profile.

**Step 1:** Configure the port profile.

```text
port-profile type vethernet [name]
switchport mode access
switchport access vlan [VLAN number]
cts manual
  policy static sgt [SGT value in hex] trusted
role-based enforcement
propagate-sgt
no shutdown
state enabled
vmware port-group
```

**Step 2:** Assign the port profile to the virtual ethernet interface.

```text
interface Vethernet [interface number]
  inherit port-profile [name]
```

As an example, this is how a server for the HR group is configured:

```text
port-profile type vethernet HR
switchport mode access
switchport access vlan 149
ccts manual
  policy static sgt 0x7d0 trusted
role-based enforcement
propagate-sgt
no shutdown
state enabled
vmware port-group
interface Vethernet8
  inherit port-profile HR
description TrustSec-HR-Server, Network Adapter 1
```
Step 3: Verify the inline configuration. You’ll see that TrustSec is in manual mode and that authorization was successful, using the SGT configured in the port profile.

```
show cts interface [interface type] [port number]
```

Example:

```
DC-N1Kv# show cts interface vethernet 8
CTS Information for Interface Vethernet8:
  CTS is enabled, mode:       CTS_MODE_MANUAL
  IFC state:                  Unknown
  Authentication Status:      CTS_AUTHC_INIT
    Peer Identity:
      Peer is:                Unknown in manual mode
      802.1X role:             CTS_ROLE_UNKNOWN
  Last Re-Authentication:
    Authorization Status:     CTS_AUTHZ_INIT
    PEER SGT:                2000
    Peer SGT assignment:     Trusted
  SAP Status:                CTS_SAP_INIT
    Configured pairwise ciphers:
    Replay protection:
    Replay protection mode:
    Selected cipher:
    Current receive SPI:
    Current transmit SPI:
    Propagate SGT: Enabled
```

Step 4: For every server you will assign an SGT, repeat this procedure.

**TrustSec across the WAN**

The campus is configured to support TrustSec, and now you extend that to remote sites across the WAN. As in the campus, there are two ways to propagate SGTs across the WAN: SXP and inline tagging. SXP over the WAN functions the same as it does in the campus. You configure SXP on the remote site router and have it peer with the access switch and WLC at the remote site and the WAN aggregation router at the campus. The remote site router propagates tags learned from the access switch and WLC to the WAN aggregation router. Configuring SXP on the access switch is covered in Procedure 1, “Configure SXP on IOS devices” and configuring SXP on the WLC is covered in Procedure 2, “Configure SXP on WLCs”.

Inline tagging over the WAN is supported in a few different mechanisms: Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport VPN (GET VPN), Generic Routing Encapsulation (GRE), and Enhanced Interior Gateway Routing Protocol Over the Top (EIGRP OTP). This design deploys DMVPN and GET VPN. The remote site access switch propagates the tag inline to the remote site router, and that tag is propagated over the WAN via encapsulation to the WAN aggregation router. Configuring inline tagging on the access switch is covered in Procedure 6, “Configure Inline tagging in IOS switches.”

**Procedure 9  **Enable SXP on ISR

Configuring SXP on the Cisco Integrated Services Router (ISR) family is the same as configuring it on Cisco Catalyst switches.

**Step 1:** Connect to the console of the router and configure SXP. The role of the device is either speaker or listener, depending on if the device is sending or receiving IP-to-SGT bindings.

```bash
cts sxp enable
cts sxp default source-ip [IP address of device]
cts sxp default password [password]
cts sxp connection peer [IP address of peer device] password default mode local [speaker|listener]
```

**Tech Tip**

The source IP address is typically the management IP address of the device or a loopback address.

An example configuration from a remote site router that is a speaker to the WAN aggregation router and a listener to an access switch.

```bash
cts sxp enable
cts sxp default source-ip 10.255.243.47
cts sxp default password [password]
cts sxp connection peer 10.5.58.5 password default mode local listener
cts sxp connection peer 10.4.32.243 password default mode local speaker
```

**Step 2:** Verify the SXP connection.

```bash
show cts sxp connections
```
Example:

```
RS47-1921#show cts sxp connections
SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: 10.255.243.47
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.4.32.243
Source IP        : 10.255.243.47
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 0:00:08:51 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.5.58.5
Source IP        : 10.255.243.47
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 0:00:12:16 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```
Step 3: For each SXP remote site router you will add, repeat this procedure.

**Procedure 10  Enable inline tagging on the ISR**

Configure the router to support inline on the link to the access switch.

**Step 1:** Connect to the console of the router and configure inline tagging.

```plaintext
interface [interface type] [port number]
  shutdown
  no cts role-based enforcement
  cts manual
  policy static sgt 2 trusted
  no shutdown
```

**Tech Tip**

To ensure the new TrustSec policy takes effect, you need to reset the interface by shutting it down and then re-enabling it. To use TrustSec in the most scalable manner, we recommend turning off enforcement on links between TrustSec-capable devices in order to ensure that filtering is done on egress from the TrustSec environment.

SGT 2 is the tag reserved for TrustSec Devices and the keyword trusted tells this switch to trust tags coming into this interface and not overwrite an existing tag.

**Procedure 11  Enable inline tagging over DMVPN**

To support inline tagging over DMVPN, you configure the GRE tunnel on both the remote site and WAN aggregation routers to add the tag to the Cisco Metadata (CMD) in the GRE payload. Support for this is determined during tunnel negotiation. The endpoints exchange capabilities using Next Hop Resolution Protocol (NHRP), and if both endpoints are configured to propagate SGTs, the tags are added. This allows you to migrate remote sites gradually to support inline tagging.

**Step 1:** Connect to the console of the router and configure inline tagging for DMVPN.

```plaintext
interface Tunnel <number>
  cts sgt inline
```

**Step 2:** Verify the inline configuration. TrustSec is enabled using an SGT of 2 on both the remote site and the WAN aggregation router.

```plaintext
show tunnel endpoints tunnel [tunnel number]
```
As an example:

```
RS15-4331#show tunnel endpoints tunnel 20
Tunnel20 running in multi-GRE/IP mode

Endpoint transport 172.18.140.20 Refcount 3 Base 0x7F3F8C7D3AC0 Create Time 00:04:07
overlay 10.6.38.1 Refcount 2 Parent 0x7F3F8C7D3AC0 Create Time 00:04:07
Tunnel Subblocks:
  Tunnel TrustSec:
    1 metadata enabled (CTS-SGT:2 )
  tunnel-nhrp-sb:
    NHRP subblock has 1 entries; TrustSec enabled; Services/Metadata: CTS-SGT

WE2-INET1-4451-1#show tunnel endpoints tunnel 20
Tunnel20 running in multi-GRE/IP mode

Endpoint transport 172.18.200.18 Refcount 3 Base 0x7FEDB2CD3DD0 Create Time 00:12:18
overlay 10.6.38.15 Refcount 2 Parent 0x7FEDB2CD3DD0 Create Time 00:12:18
Tunnel Subblocks:
  tunnel-qos (Extend Forwarding):
    Tunnel-QoS subblock, QoS policy applied: RS-GROUP-20MBPS-POLICY
overlay 10.6.38.15 Refcount 2 Parent 0x7FEDB2CD3DD0 Create Time 00:12:18
Tunnel Subblocks:
  tunnel-nhrp-sb:
    NHRP subblock has 1 entries; TrustSec enabled; Services/Metadata: CTS-SGT
  Tunnel TrustSec:
    1 metadata enabled (CTS-SGT:2 )
```
Procedure 12  Enable inline tagging over GET VPN

To support inline tagging over GET VPN, you configure the key server to add the tag to the Cisco Metadata (CMD) in the IPSec payload. When the key server receives a request from a group member router, the tagging capability is negotiated. If both endpoints are configured to propagate SGTs, the tags are added. This allows you to migrate remote sites gradually to support inline tagging.

Step 1: Connect to the console of the router and configure inline tagging for GET VPN.

```
crypto gdoi group [group name]
    server local
    sa ipsec [sequence number]
        tag cts sgt
```

Example:

```
crypto gdoi group GETVPN-GROUP
    identity number 65511
    server local
        rekey algorithm aes 256
        rekey retransmit 40 number 3
        rekey authentication mypubkey rsa GETVPN-REKEY-RSA
        rekey transport unicast
    sa ipsec 10
        profile GETVPN-PROFILE
            match address ipv4 GETVPN-POLICY-ACL
            replay time window-size 20
            tag cts sgt
        address ipv4 10.4.32.1 52
        redundancy
            local priority 75
            peer address ipv4 10.4.32.151
```

Tech Tip

The configuration for inline tagging support is applied at the group level for GET VPN and enables the feature for every group member. If you want to migrate remote sites you need to create another group that supports inline tagging and move remote sites from the original group to this new group.
**Step 2:** Connect to the console of the remote site router and verify the inline configuration. You’ll see the tag method is using SGTs.

```
show crypto gdoi
```

**Step 3:** As an example (output edited for brevity):

```
RS35-4331#show crypto gdoi

GROUP INFORMATION

<table>
<thead>
<tr>
<th>Group Name</th>
<th>GETVPN-GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Identity</td>
<td>65511</td>
</tr>
<tr>
<td>Group Type</td>
<td>GDOI (ISAKMP)</td>
</tr>
<tr>
<td>Crypto Path</td>
<td>ipv4</td>
</tr>
<tr>
<td>Key Management Path</td>
<td>ipv4</td>
</tr>
<tr>
<td>Rekeys received</td>
<td>99</td>
</tr>
<tr>
<td>IPSec SA Direction</td>
<td>Both</td>
</tr>
</tbody>
</table>

Group Server list : 10.4.32.151
10.4.32.152

<Output deleted>

TEK POLICY for the current KS-Policy ACEs Downloaded:

GigabitEthernet0/0/0:

IPsec SA:

**spi:** 0xA1B3796E(2712893806)
KGS: Disabled
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (5766)
Anti-Replay(Time Based): 20 sec interval
tag method : cts sgt
alg key size: 32 (bytes)
sig key size: 20 (bytes)
encaps: ENCAPS_TUNNEL

IPsec SA:

**spi:** 0xFBDEC3C6(4225680326)
The TrustSec policy has been configured and the infrastructure has been configured to propagate tags throughout the network. The next step is to enable enforcement in the data center. There are two places where enforcement can be enabled. The first is on the Nexus 7000 switches used for the data center core. The other is on the Cisco ASA firewalls in the data center.

**Procedure 1** Configure Nexus 7000 for enforcement

**Step 1:** To obtain the policy from Cisco ISE, the Nexus 7000 switches need to be authenticated and authorized. This was configured in Procedure 1, “Enable TrustSec on NX-OS Switches”.

**Step 2:** Connect to the console of the switch and enable TrustSec enforcement and counters.

```bash
ccts role-based counters enable
ccts role-based enforcement
```

**Step 3:** Verify the policy is downloaded.

```bash
show ccts role-based policy
```

This shows the entire policy. To show a portion of the policy, you can add the source tag, the destination tag, or both.

```bash
show ccts role-based policy sgt [source tag number]
show ccts role-based policy dgt [destination tag number]
show ccts role-based policy sgt [source tag number] dgt [destination tag number]
```
Example:

```
DC-N7004-2# show cts role-based policy sgt 4001 dgt 4000

sgt:4001(Research_Users)
dgt:4000(Research_Servers)    rbacl:Research_ACL
    permit ip log

DC-N7004-2# show cts role-based policy sgt 4001 dgt 3000

sgt:4001(Research_Users)
dgt:3000(IT_Servers)         rbacl:Deny_All
    deny ip log
```

**Procedure 2**  
**Configure Cisco ASA for enforcement**

Cisco ASA allows you to use SGTs in the firewall policy rules. You configured the appliance to retrieve the Trust-Sec environment data, which is the table of SGT names and numbers, in Procedure 4, "Configure SXP on Cisco ASA," and you configure firewall rules using this data. In this deployment, the appliance provides more granular enforcement than what is being done on the Cisco Nexus 7000 switches by limiting access to the servers to allow only web traffic and ICMP from the users.

**Step 1:** In a browser, navigate to the Cisco ASA management console (example: https://DC-ASA5585X.cisco.local), and then click *Run ASDM*.

**Step 2:** If you are using virtual contexts on your firewall, in the Device List, choose the context.
Step 3: To verify the TrustSec environment data has been downloaded, navigate to Monitoring > Properties > Identity by TrustSec > Environment Data.

Step 4: Navigate to Configuration > Firewall > Access Rules.

Step 5: Click Add.

Step 6: Select interface outside and the Action permit.

Step 7: In the Source criteria section, in the Security Group field, click the ellipsis (...). The Browse Security Group window opens.
Step 8: In the Existing Security Group section, locate the user group you want to configure (example: Research_Users), and then click Add.

Step 9: Click OK. The window closes.

Step 10: In the Destination criteria section, in the Security Group field, click the ellipsis (...). The Browse Security Group window opens.

Step 11: In the Existing Security Group section, locate the user group you want to configure (example: Research_Servers), and then click Add. Click OK. The window closes.

Step 12: In the Service field, click the ellipsis (...). The Browse Service window opens.
Step 13: Select the services you want to permit. (Examples: tcp/http, tcp/https, icmp/echo)

Step 14: Click OK. The window closes.

Step 15: Select Enable Logging, and then click OK.
Step 16: For each rule you will configure, repeat Step 4 through Step 15.

Step 17: Click Apply, and then click Save.
# Appendix A: Product List

## IDENTITY MANAGEMENT

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

## DATA CENTER

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Switch</td>
<td>Cisco Nexus 7000 Series 4-Slot Chassis</td>
<td>N7K-C7004</td>
<td>NX-OS 7.3(0)D1(1)</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 7000 - Supervisor 2</td>
<td>N7K-SUP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 7000 F2-Series 48 Port 1/10G (SFP+) Enhanced</td>
<td>N7K-F248XP-25E</td>
<td></td>
</tr>
<tr>
<td>Distribution Switch</td>
<td>Cisco Nexus 5672UP 1RU, 32 p 10-Gbps SFP+, 16 Unified Ports, 6p 40G QSFP+</td>
<td>N5K-C5672UP</td>
<td>NX-OS 7.1(0) N1(1b)</td>
</tr>
<tr>
<td></td>
<td>Nexus 5600 VM-FEX license</td>
<td>N56-VMFEX9</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix A: Product List

### Ethernet Extension

<table>
<thead>
<tr>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender</td>
<td>N2K-C2248TP-E</td>
<td></td>
</tr>
<tr>
<td>Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender</td>
<td>N2K-C2248TP-1GE</td>
<td></td>
</tr>
<tr>
<td>Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender</td>
<td>N2K-C2232PP-10GE</td>
<td></td>
</tr>
</tbody>
</table>

### Firewall

<table>
<thead>
<tr>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA 5585-X Security Plus Firewall Edition SSP-20 bundle includes 8 Gigabit Ethernet interfaces, 2 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, 3DES/AES license</td>
<td>ASA5585-S20X-K</td>
<td>9.4(1), ASDM 7.4(1)</td>
</tr>
<tr>
<td>Cisco ASA 5585-X Security Services Processor-20 with firewall services, 10,000 IPsec VPN peers, 2 SSL VPN peers, 8 Gigabit Ethernet interfaces, 2 Gigabit Ethernet SFP interfaces, DES</td>
<td>ASA-SSP-20-K8</td>
<td></td>
</tr>
<tr>
<td>Cisco ASA 5585-X Security Plus License</td>
<td>ASA5585-SEC-PL</td>
<td></td>
</tr>
<tr>
<td>Cisco ASA 5500 5 Security Contexts License</td>
<td>A5500-SC-5</td>
<td></td>
</tr>
<tr>
<td>Cisco ASA 5500 10 Security Contexts License</td>
<td>A5500-SC-10</td>
<td></td>
</tr>
<tr>
<td>Cisco ASA 5500 20 Security Contexts License</td>
<td>A5500-SC-20</td>
<td></td>
</tr>
<tr>
<td>Cisco ASA 5500 50 Security Contexts License</td>
<td>A5500-SC-50</td>
<td></td>
</tr>
</tbody>
</table>

### Data Center Virtualization

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Switch</td>
<td>Cisco Nexus 1000v Advanced Edition CPU License 1-pack</td>
<td>N1K-VLCPU-01=</td>
<td>5.2(1)SV3(1.15)</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000v Advanced Edition CPU License 4-pack</td>
<td>N1K-VLCPU-04=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000v Advanced Edition CPU License 16-pack</td>
<td>N1K-VLCPU-16=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000v Advanced Edition CPU License 32-pack</td>
<td>N1K-VLCPU-32=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000v Advanced Edition CPU License 64-pack</td>
<td>N1K-VLCPU-64=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000v Advanced Edition CPU License 128-pack</td>
<td>N1K-VLCPU-128=</td>
<td></td>
</tr>
<tr>
<td>VMWare</td>
<td>ESXi</td>
<td>ESXi</td>
<td>5.5</td>
</tr>
<tr>
<td></td>
<td>VMware vSphere</td>
<td>ESXi</td>
<td></td>
</tr>
</tbody>
</table>
# LAN ACCESS LAYER

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modular Access Layer Switch</strong></td>
<td>Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot</td>
<td>WS-C4507R+E</td>
<td>3.6.4.E(15.2.2E4) IP Base license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps</td>
<td>WS-X45-SUP8-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module</td>
<td>WS-X4712-SFP+E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)</td>
<td>WS-X4748-RJ45V+E</td>
<td></td>
</tr>
<tr>
<td><strong>Stackable Access Layer Switch</strong></td>
<td>Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports</td>
<td>WS-C3850-48F</td>
<td>3.6.4.E(15.2.2E4) IP Base license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports</td>
<td>WS-C3850-24P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series 2 x 10GE Network Module</td>
<td>C3850-NM-2-10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series 4 x 1GE Network Module</td>
<td>C3850-NM-4-1G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink</td>
<td>WS-C3650-24PD</td>
<td>3.6.4.E(15.2.2E4) IP Base license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink</td>
<td>WS-C3650-24PS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3650 Series Stack Module</td>
<td>C3650-STACK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 2960-X Series 24 10/100/1000 Ethernet and 2 SFP+ Uplink</td>
<td>WS-C2960X-24PD</td>
<td>15.2(3)E1 LAN Base license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module</td>
<td>C2960X-STACK</td>
<td></td>
</tr>
<tr>
<td><strong>Standalone Access Layer Switch</strong></td>
<td>Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink</td>
<td>WS-C3650-24PS</td>
<td>3.6.4.E(15.2.2E4) IP Base license</td>
</tr>
</tbody>
</table>
## LAN DISTRIBUTION LAYER

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular Distribution Layer Virtual Switch Pair</td>
<td>Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis</td>
<td>C6807-XL</td>
<td>15.2(1)SY1</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4</td>
<td>VS-S2T-10G</td>
<td>Enterprise Services license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4</td>
<td>WS-X6904-40G-2T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module</td>
<td>CVR-CFP-4SFP10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6800 32 port 10GE with integrated dual DFC4</td>
<td>C6800-32P10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 Distributed Forwarding Card 4</td>
<td>WS-F6K-DFC4-E</td>
<td></td>
</tr>
</tbody>
</table>

| Modular Distribution Layer Virtual Switch Pair | Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot | WS-C4507R+E | 3.6.4.E(15.2.2E4) |
| | Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps | WS-X45-SUP7-E | Enterprise Services license |
| | Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module | WS-X4712-SFP+E | |
| | Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45) | WS-X4748-RJ45V+E | |

| Fixed Distribution Layer Virtual Switch Pair | Cisco Catalyst 4500-X Series 32 Port 10GbE IP Base Front-to-Back Cooling | WS-C4500X-32SFP+ | 3.6.4.E(15.2.2E4) |

| Stackable Distribution Layer Switch | Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet | WS-C3850-12S | 3.6.4.E(15.2.2E4) |

## LAN CORE LAYER

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular Core Layer Virtual Switch Pair</td>
<td>Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis</td>
<td>C6807-XL</td>
<td>15.2(1)SY1</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4</td>
<td>VS-S2T-10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4</td>
<td>WS-X6904-40G-2T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 Distributed Forwarding Card 4</td>
<td>WS-F6K-DFC4-E</td>
<td></td>
</tr>
</tbody>
</table>
### LAN DISTRIBUTION – SERVICES BLOCK

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular Distribution Layer Virtual Switch Pair</td>
<td>Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis</td>
<td>C6807-XL</td>
<td>15.2(1)SY1 IP Services license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4</td>
<td>VS-S2T-10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4</td>
<td>WS-X6904-40G-2T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module</td>
<td>CVR-CFP-4SFP10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6800 32 port 10GE with integrated dual DFC4</td>
<td>C6800-32P10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 6500 Distributed Forwarding Card 4</td>
<td>WS-F6K-DFC4-E</td>
<td></td>
</tr>
</tbody>
</table>

### WIRELESS LAN CONTROLLERS

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Site Controller</td>
<td>Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points</td>
<td>AIR-CT7510-6K-K9</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points</td>
<td>AIR-CT7510-3K-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points</td>
<td>AIR-CT7510-2K-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 7500 Series Wireless Controller for up to 1000 Cisco access points</td>
<td>AIR-CT7510-1K-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 7500 Series Wireless Controller for up to 500 Cisco access points</td>
<td>AIR-CT7510-500-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 7500 Series Wireless Controller for up to 300 Cisco access points</td>
<td>AIR-CT7510-300-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 7500 Series High Availability Wireless Controller</td>
<td>AIR-CT7510-HA-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Virtual Wireless Controller for up to 5 Cisco access points</td>
<td>L-AIR-CTVM-5-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Virtual Wireless Controller 25 Access Point Adder License</td>
<td>L-LIC-CTVM-25A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Virtual Wireless Controller 5 Access Point Adder License</td>
<td>L-LIC-CTVM-5A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Virtual Wireless Controller 1 Access Point Adder License</td>
<td>L-LIC-CTVM-1A</td>
<td></td>
</tr>
<tr>
<td>On Site, Remote Site, or Guest Controller</td>
<td>Cisco 5520 Series Wireless Controller for up to 50 Cisco access points</td>
<td>AIR-CT5520-50-K9</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 5520 Wireless Controller 100 AP License</td>
<td>LIC-CTS5520-100A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5520 Wireless Controller 50 AP License</td>
<td>LIC-CTS5520-50A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5520 Wireless Controller 1 AP Adder License</td>
<td>LIC-CT5520-1A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for up to 500 Cisco access points</td>
<td>AIR-CT5508-500-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for up to 250 Cisco access points</td>
<td>AIR-CT5508-250-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for up to 100 Cisco access points</td>
<td>AIR-CT5508-100-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for up to 50 Cisco access points</td>
<td>AIR-CT5508-50-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for up to 25 Cisco access points</td>
<td>AIR-CT5508-25-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for up to 12 Cisco access points</td>
<td>AIR-CT5508-12-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 5500 Series Wireless Controller for High Availability</td>
<td>AIR-CT5508-HA-K9</td>
<td></td>
</tr>
<tr>
<td>On Site Controller, Guest Controller</td>
<td>Cisco 2500 Series Wireless Controller for up to 50 Cisco access points</td>
<td>AIR-CT2504-50-K9</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 2500 Series Wireless Controller for up to 25 Cisco access points</td>
<td>AIR-CT2504-25-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 2500 Series Wireless Controller for up to 15 Cisco access points</td>
<td>AIR-CT2504-15-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 2500 Series Wireless Controller for up to 5 Cisco access points</td>
<td>AIR-CT2504-5-K9</td>
<td></td>
</tr>
</tbody>
</table>
## WIRELESS LAN ACCESS POINTS

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Access Points</td>
<td>Cisco 3700 Series Access Point 802.11ac and CleanAir with Internal Antennas</td>
<td>AIR-CAP3702I-x-K9</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 3700 Series Access Point 802.11ac and CleanAir with External Antenna</td>
<td>AIR-CAP3702E-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas</td>
<td>AIR-CAP3602I-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas</td>
<td>AIR-CAP3602E-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas</td>
<td>AIR-CAP2602I-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas</td>
<td>AIR-CAP2602E-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with Internal Antennas</td>
<td>AIR-CAP1602I-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with External Antennas</td>
<td>AIR-CAP1602E-x-K9</td>
<td></td>
</tr>
</tbody>
</table>

## WIRELESS LAN

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless LAN</td>
<td>Cisco 802.11ac Wave 1 Module for 3600 Series Access Point</td>
<td>AIR-RM3000AC-x-K9=</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 802.11ac Wave 1 Module for 3600 Series Access Point 10 Pack</td>
<td>AIR-RM3000ACxK910=</td>
<td></td>
</tr>
</tbody>
</table>

## WAN AGGREGATION

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN-aggregation Router</td>
<td>Cisco Aggregation Services 1002X Router</td>
<td>ASR1002X-5G-VPNK9</td>
<td>IOS-XE 03.16.01a.S Advanced Enterprise</td>
</tr>
<tr>
<td></td>
<td>Cisco Aggregation Services 1001X Router</td>
<td>ASR1001X-5G-VPN</td>
<td>IOS-XE 03.16.01a.S Advanced Enterprise</td>
</tr>
<tr>
<td></td>
<td>Cisco ISR 4451-X Security Bundle with SEC License</td>
<td>ISR4451-X-SEC/K9</td>
<td>IOS-XE 03.16.01a.S securityk9</td>
</tr>
</tbody>
</table>
### WAN REMOTE SITE

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular WAN</td>
<td>Remote-site Router</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 4451 AX Bundle with APP and SEC License</strong></td>
<td>ISR4451-X-AX/K9</td>
<td><strong>IOS-XE 03.16.01a.S</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, appxk9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 4431 AX Bundle with APP and SEC License</strong></td>
<td>ISR4431-AX/K9</td>
<td><strong>IOS-XE 03.16.01a.S</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, appxk9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 4351 AX Bundle with APP and SEC License</strong></td>
<td>ISR4351-AX/K9</td>
<td><strong>IOS-XE 03.16.01a.S</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, appxk9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 4331 AX Bundle with APP and SEC License</strong></td>
<td>ISR4331-AX/K9</td>
<td><strong>IOS-XE 03.16.01a.S</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, appxk9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 4321 AX Bundle with APP and SEC License</strong></td>
<td>ISR4321-AX/K9</td>
<td><strong>IOS-XE 03.16.01a.S</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, appxk9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 3945 AX Bundle with APP and SEC License</strong></td>
<td>C3945-AX/K9</td>
<td><strong>15.5(3)M1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, datak9, uck9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 3925 AX Bundle with APP and SEC License</strong></td>
<td>C3925-AX/K9</td>
<td><strong>15.5(3)M1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, datak9, uck9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 2951 AX Bundle with APP and SEC License</strong></td>
<td>C2951-AX/K9</td>
<td><strong>15.5(3)M1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, datak9, uck9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 2921 AX Bundle with APP and SEC License</strong></td>
<td>C2921-AX/K9</td>
<td><strong>15.5(3)M1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, datak9, uck9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 2911 AX Bundle with APP and SEC License</strong></td>
<td>C2911-AX/K9</td>
<td><strong>15.5(3)M1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, datak9, uck9</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ISR 1941 AX Bundle with APP and SEC License</strong></td>
<td>C1941-AX/K9</td>
<td><strong>15.5(3)M1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>securityk9, datak9</strong></td>
</tr>
</tbody>
</table>
Please use the feedback form to send comments and suggestions about this guide.