



Cisco TrustSec How-To Guide: ISE Deployment Types and Guidelines

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Table of Contents	1
Introduction	3
What Is the Cisco TrustSec System?	3
About the TrustSec How-To Guides.....	3
<i>What does it mean to be 'TrustSec Certified'?</i>	4
Understanding ISE Deployment	5
ISE Personas (Service Node Types)	5
Types of Deployment.....	5
<i>Standalone</i>	5
<i>Basic 2-Node (Redundant) Deployment: Up to 2,000 Endpoints</i>	6
<i>Distributed Deployment: 2,000 to 10,000 Endpoints</i>	7
<i>Distributed Deployment: Up to 100,000 Endpoints (Maximum)</i>	8
Adding a Secondary Node for Distributed Deployment.....	9
<i>Basic ISE Configuration for Distributed Deployment</i>	10
Determining the Minimum Appliance Quantity and Platform.....	13
Communication Between Personas	14
Bandwidth Requirements for Distributed Deployments.....	15
Appendix A: References	17
Cisco TrustSec System:.....	17
Device Configuration Guides:	17

Introduction

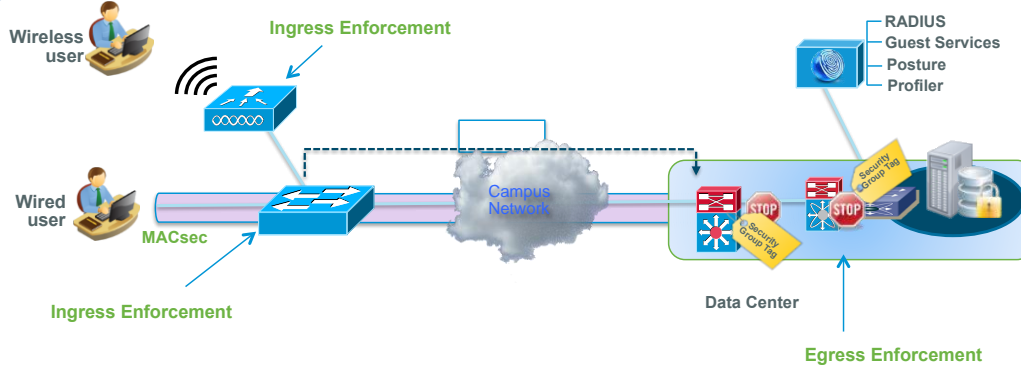
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

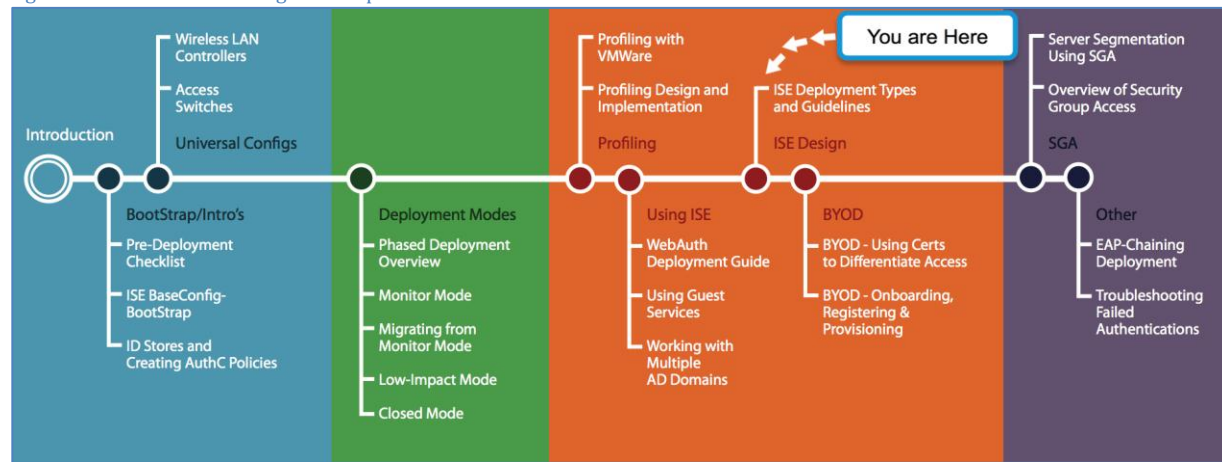


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide in this series comes with a subway-style “You Are Here” map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked “TrustSec certified,” all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as “TrustSec certified”. The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.





Understanding ISE Deployment

The number of possible endpoints supported by Cisco TrustSec is the single most important aspect of Cisco ISE design. Cisco ISE version 1.1.1 supports up to 100,000 concurrent endpoints. Policy Service Node (PSN) deployment varies based on the number of endpoints—for example, whether your network has 500 wireless endpoints or 80,000 concurrent endpoints. Your admin and monitoring nodes can be consolidated centrally. This document highlights rules and design requirements to build such centralized or distributed ISE deployments.

ISE Personas (Service Node Types)

Cisco ISE's primary purpose is to provide all-in-one policy management infrastructure for basic authentication, authorization, and auditing. It also offers advanced services such as profiler, guest management, and posture assessment services to manage the entire lifecycle of network access. A standalone ISE appliance (or virtual machine appliance) can provide this “all-in-one” functionality for small deployments. In midsize to large enterprise deployments, ISE functions can be divided into several dedicated service nodes called “personas.” The main goal of dividing into dedicated service nodes is to distribute the load and traffic caused by authentication services, and to avoid points of failure by centralizing service in one appliance. Following is a summary of ISE personas (service nodes).

Table 1 Type of ISE Personas

	Administration	Allows you to perform all administrative operations on Cisco ISE. Also called “Policy Administration Node (PAN)”
	Policy Service	Provides network access (AAA runtime engine), posture, guest access, and profiling services. Also called “Policy Service Node (PSN)”
	Monitoring	Enables Cisco ISE to function as the log collector and store log messages from the administration and policy service personas. Also called “Monitoring Node (MNT)”
	Inline Posture	A gatekeeping node that is positioned behind the network access device (e.g., WLC, VPN concentrator) to provide inline posture service. Also called “Inline Posture Node (IPN)”

Each service node has its own responsibility but is integrated seamlessly regardless of how the nodes are distributed. Figure 23 illustrates how the service nodes communicate with each other.

Note: The Policy Service Node provides user services, including RADIUS/AAA, sponsor/guest portal, profiling probing, and posture assessment. The Inline Posture Node is dedicated to inline posture service. You will not be able to mix ISE nodes (PAN, MNT, and PSN) with Inline Posture Nodes.

Types of Deployment

There are several ways to deploy an ISE solution, based on the number of concurrent endpoints in the deployment.

Standalone

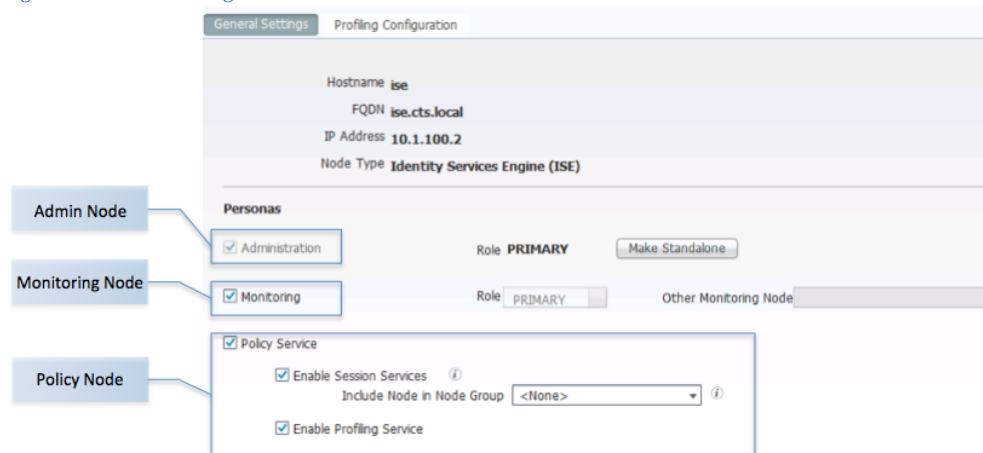
Standalone deployment is the simplest deployment type, consisting of one ISE appliance or a virtual appliance. All personas (PAN, MNT, and PSN) are running on the same appliance, as shown in Figure 3. One standalone ISE node supports up to 2,000 endpoints. This number remains the same regardless of ISE appliance type (e.g., ISE-3315 or ISE-3395).

Figure 3 Standalone Node



Figure 4 shows a screen capture of ISE node configuration (Menu → Administration → System → Deployment → your_ise_hostname). If the deployment is standalone (by default), all personas should be selected.

Figure 4 ISE Node Configuration

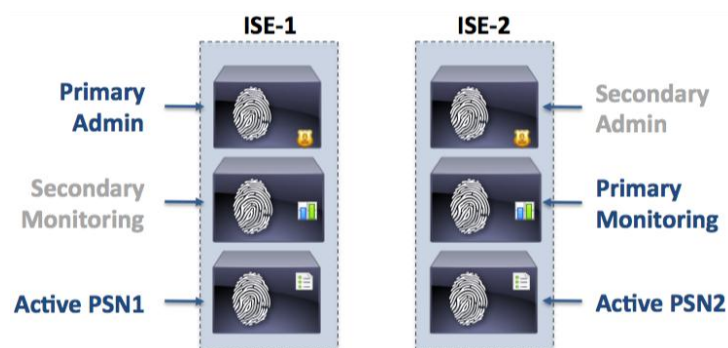


Basic 2-Node (Redundant) Deployment: Up to 2,000 Endpoints

Standalone deployment is useful when you are testing a solution in the lab, as you can test all services in a single appliance. For any deployment in a production network, however, redundant ISEs are recommended in case one ISE fails. When ISE appliances form redundancy, you can configure them to serve as primary and secondary nodes for administration and monitoring services. Having a single primary administration node and multiple secondary nodes is sometime referred as an ISE distributed deployment.

Figure 5 shows a configuration where ISE-1 serves as the primary PAN and the secondary MNT. ISE-2 serves as the secondary PAN and the primary MNT. By balancing primary and secondary service roles, your traffic load can be balanced while maintaining high availability. With redundant ISEs, the maximum number of endpoints should be 2,000.

Figure 5 Basic 2-Node Deployment Persona Assignment

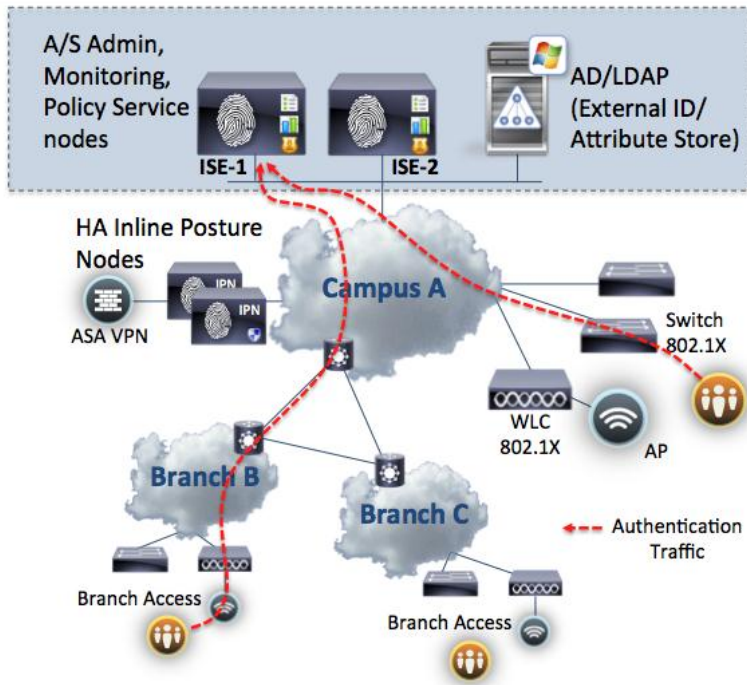


This type of deployment is common in SMB environments. Since all personas are running on a pair of centrally located ISE appliances (in headquarters or a data center), your authentication, profiling, posture, and guest services are centralized, as is your policy service. Because your PSNs are running on the same ISEs, all service traffic, including 802.1X authentication from wired and wireless devices in campus and branch networks, is served by those ISEs.

Keep in mind that your branch office does not have a local PSN, so if the WAN link goes down and branch switches or Wireless LAN Controllers (WLCs) cannot reach the ISEs, an authentication service outage is possible. Make sure that your 802.1X network design includes fail-open scenarios with features such as Inaccessible Authentication Bypass (for switches) and Local Extensible Authentication Protocol (EAP; for wireless).

Figure 6 depicts a centralized ISE deployment.

Figure 6 Centralized ISE Deployment



Distributed Deployment: 2,000 to 10,000 Endpoints

A 2-node deployment gives you a basic idea of how each persona can be configured in redundant mode. When deployment needs to support 2,000–10,000 endpoints, we recommend detaching the PSN from the PAN or MNT so that the PSN resources can serve a higher number of network access requests from endpoints.

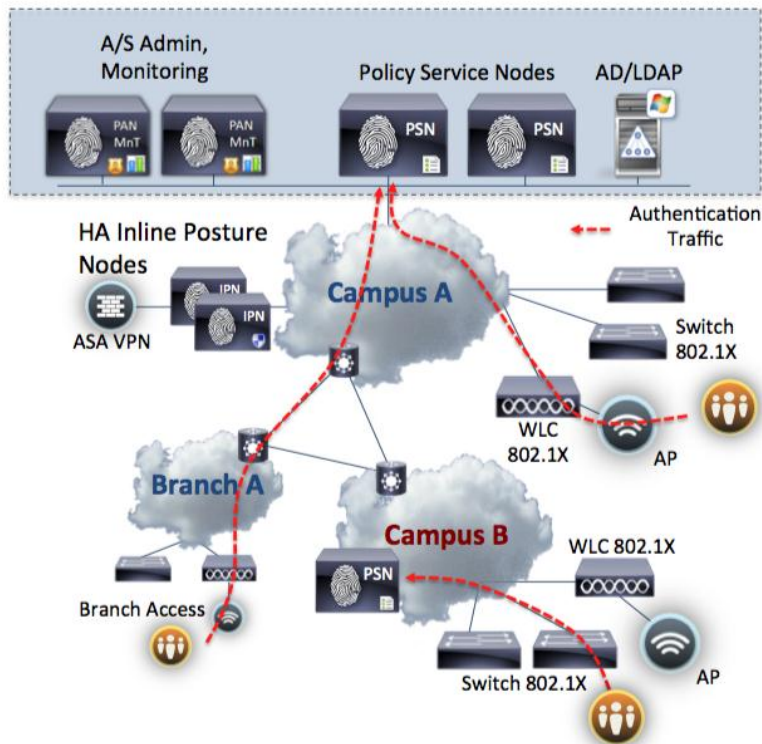
In this type of distributed deployment, we recommend two sets of Cisco ISE nodes for admin and monitoring functions and up to five PSNs, as shown in Figure 7. Separating the runtime engine (PSN) and administrative personas (PAN and MNT) also allows each PSN to handle more endpoints.

Figure 7 Distributed Deployment (2,000 to 10,000 Endpoints)



Figure 8 illustrates a typical distributed deployment with a pair of PANs/MNTs and distributed PSNs. This deployment type is effective when you have more than two larger sites that require dedicated runtime to process all authentication and service requests, while centralized PSNs continue to serve requests from smaller branch offices.

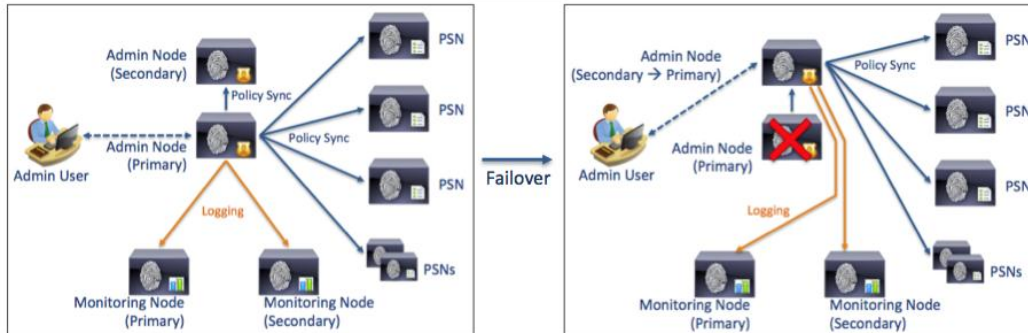
Figure 8 Distributed Deployment (2,000 to 10,000 Endpoints) Topology Example



A Cisco ISE operator uses the centralized primary PAN to manage all the policies. The configuration and policies are synchronized between the primary node and all other nodes whenever changes are made via the primary node. As shown in Figure 9, upon failure of the primary node, the admin user can connect to the secondary node; all changes via backup PAN are automatically synchronized to all PSNs.

Note: The secondary PAN must be manually promoted to the primary role whenever the primary node goes down.

Figure 9 Failover Between Primary and Secondary Administration Nodes



If you have more than two PSNs in single location, you can cluster those PSNs behind a load-balancing device (such as a Cisco Application Control Engine) for better performance. Additionally, other network access devices (NADs), such as ones in the second campus network, can point to the headquarter PSN as a secondary RADIUS server for high-availability purposes.

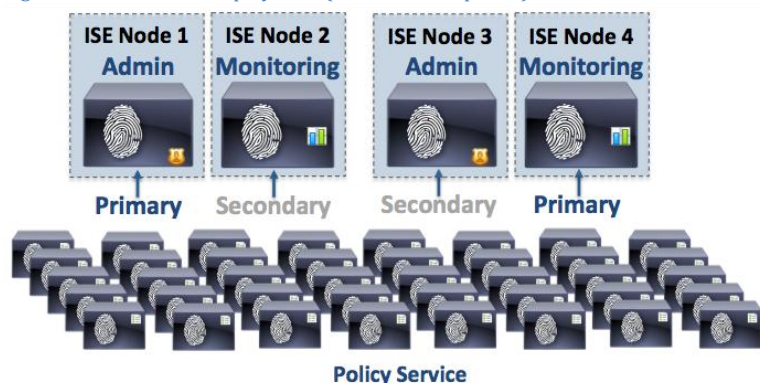
Distributed Deployment: Up to 100,000 Endpoints (Maximum)

Most midsize to large enterprises can easily go over the 10,000 concurrent endpoint limit, especially with all the BYOD devices coming onboard. Cisco ISE Version 1.1.1 currently supports up to 100,000 concurrent endpoints. In order to support this high number of endpoints and maintain performance, the Cisco ISE roles need to be separated to dedicated appliances.

Imagine that you are going to have 100,000 endpoints accessing your network, and each session generates a good amount of logs. ISE keeps all of those logs in the database to correlate events and to keep session information. In order to have better processing performance, the MNT persona needs to be separated from the PAN persona.

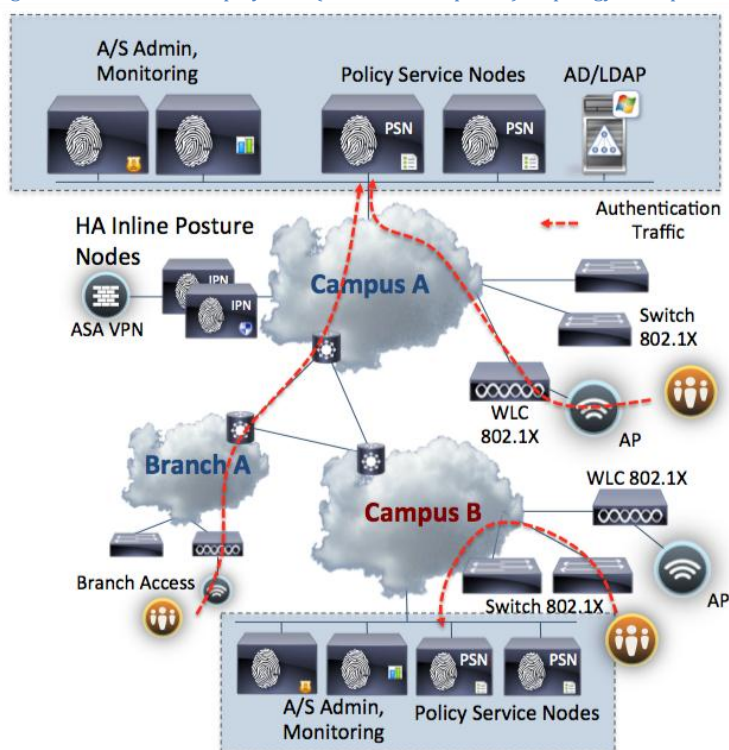
ISE supports up to two dedicated PANs and two dedicated MNTs. Each dedicated appliance can serve as primary and secondary node to maintain resiliency in case of service failure. When these nodes are separated on dedicated appliances, the number of supported PSNs also increases. With 2x PANs and 2x MNTs, ISE supports up to 40 PSNs, supporting 100,000 endpoints concurrently.

Figure 10 Distributed Deployment (~100,000 Endpoints)



Since each persona now runs on dedicated, independent nodes, those nodes can reside in a single location, or can be distributed (placed in different locations). If your company has a single data center, primary and secondary PANs and MNTs can be connected in different segments. With multiple data centers, it is more common to separate those personas in each data center location for disaster recovery (DR) purposes. Of course, the personas communicate with each other to synchronize endpoint data, session information and state, and configuration changes. With distributed personas, it is important to understand the types of communication between nodes to prevent a node from going out of sync. This will be discussed in greater detail later in this document.

Figure 11 Distributed Deployment (~100,000 Endpoints) Topology Example



Adding a Secondary Node for Distributed Deployment

In the previous section, we discussed deployment options based on deployment size. Now, let's take a look at how we add (register) a second ISE node to the existing standalone node to form a high-availability configuration. The deployment guide located at the following URL provides guidelines on setting up a distributed deployment. Please read the guidelines carefully.

http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_dis_deploy.html#wp1059169

Before you register your second ISE node to the primary node, the following must be completed:

- On both primary and secondary ISE nodes, use **ping** and **nslookup** to see whether the server's fully qualified domain names (FQDNs) are DNS-resolvable. If they are not resolvable, node registration will fail. You can perform this operation under Operation → Troubleshoot → Diagnostic Tools → General Tools → Connectivity Tests, or you can use **ping** or **nslookup** commands in the ISE CLI console.
- Make sure that all ISE nodes are running same version of code.
- The database passwords of the primary and secondary nodes should be the same. If they are different, use the following CLI commands to modify them.

```
application reset-passwd ise internal-database-admin
application reset-passwd ise internal-database-user
```

- To register and configure the secondary node, you must have either the super admin or system admin role.
- Primary node Certificate Trust List (CTL) must be populated with the appropriate Certificate Authority (CA) certificates that can be used to validate the HTTPS certificate of the secondary node.

Basic ISE Configuration for Distributed Deployment

Procedure 1 Change Standalone Role to Primary Role

Step 1 Make sure you have gone through the guidelines and prerequisites listed above.

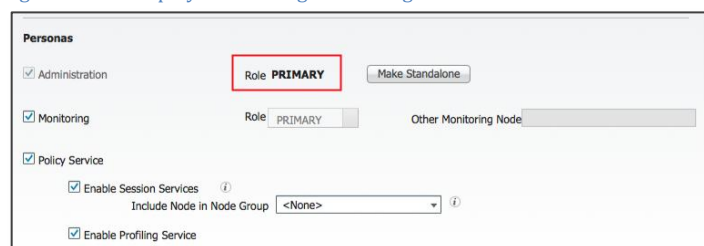
Step 2 Make sure that your first ISE node is configured with a server certificate signed by either your own CA or a third-party CA. You can check certificates for both ISE and CA under Administration → System → Certificates → Local Certificates OR Certificate Authority Certificates.

Figure 12 ISE Certificate Authority Certificate Configuration Page



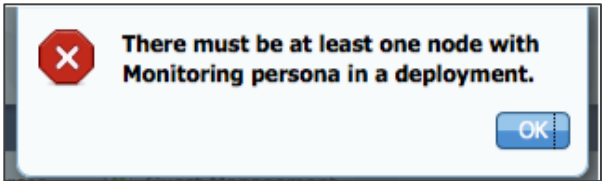
Step 3 Go to Administration → System → Deployment → <your_ise_node>. In the General Settings, under the Personas setting, click the Make Primary button. Your role should change to PRIMARY from STANDALONE. Most of the option settings will become active except the administration option, as the primary node needs to be an administration node.

Figure 13 ISE Deployment Configuration Page



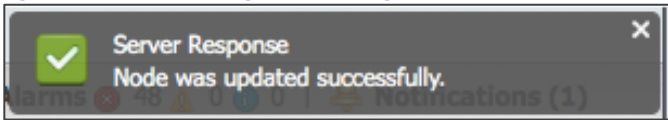
Step 4 Select Persona Type as needed. Because this is the primary node and no other node is currently registered, you must select Monitoring Personas on the primary node until the other node registers as the primary node. Otherwise, you will see the warning shown in Figure 14 when you deselect Monitoring Node and try to save the configuration.

Figure 14 Error Message



Step 5 Click the Save button. You will see the message shown in Figure 15 at bottom of your screen confirming your node type is updated successfully.

Figure 15 Successful Configuration Message



Note: When you select or deselect the policy service persona and save it, ISE must restart its application server. You are going to be logged out of the web interface for up to 10 minutes.

Step 6 If you go back to the Deployment Nodes list, you will see a table similar to the one in Figure 16. Note that the Role(s) column changed to PRI (A), PRI (M). This means this server is now the primary node for administration and monitoring.

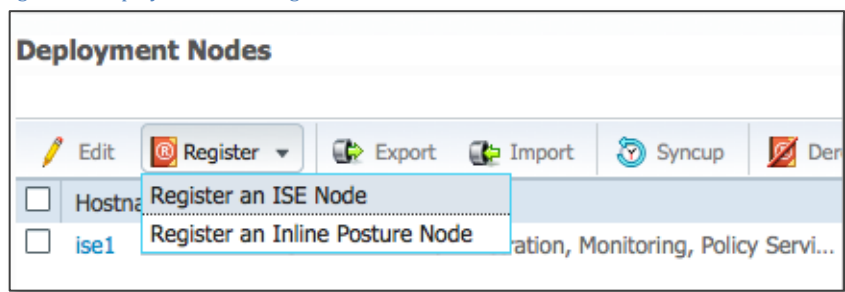
Figure 16 Deployment Node Table

Deployment Nodes							
<div>✎ Edit Ⓜ Register ➡ Export ⬅ Import ↻ Syncup 🚫 Deregister</div>							
<input type="checkbox"/>	Hostname	Node Type	Personas	Role(s)	Services	Replication Status	Sync Status
<input type="checkbox"/>	ise	ISE	Administration, Monitoring, Policy Servi...	PRI(A), PRI(M)	All	Not Applicable	Not Applicable

Procedure 2 Add Secondary Node to Primary Node

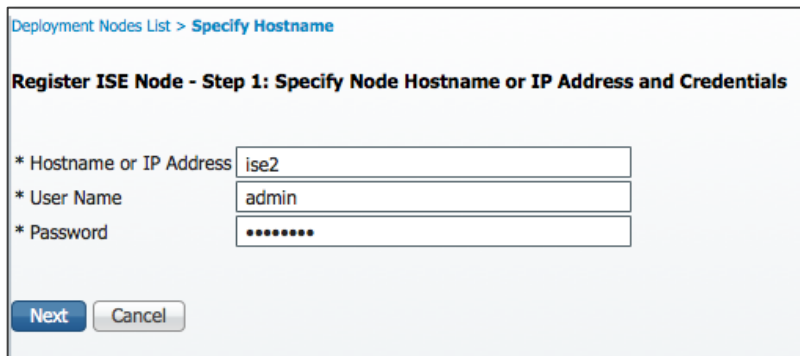
Step 1 Once you change standalone node to primary node, you can add another standalone ISE node to the primary node as a secondary node. In the Deployment Nodes screen of your primary ISE node web console, click Register. Then, click Register an ISE Node.

Figure 17 Deployment Node Registration



Step 2 You will move to the ISE node registration page. Enter the hostname or IP address of your secondary node, then the user name (typically Super Admin or System Admin role) and password. You can use the simple hostname, FQDN, or IP address of the secondary node.

Figure 18 ISE Node Registration Configuration



Note: The primary ISE node tries to communicate with this new ISE node on GigabitEthernet 0 interface (Management Interface) and authenticate using HTTPS. The primary node's Certificate Trust List (CTL) must be populated with the appropriate CA certificates that can be used to validate the HTTPS certificate of the secondary node. In addition, both primary and secondary nodes need to be DNS-resolvable.

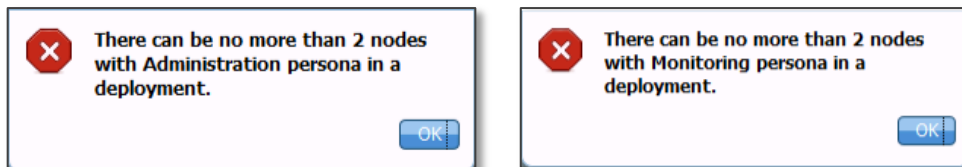
Step 3 Once your secondary ISE is contacted, it will be registered as the secondary node. Click Save to complete the registration process.

Procedure 3 Troubleshooting

You can create another standalone ISE node and register to the primary ISE node. (This will be your third ISE node.) There are some additional considerations when registering the third node:

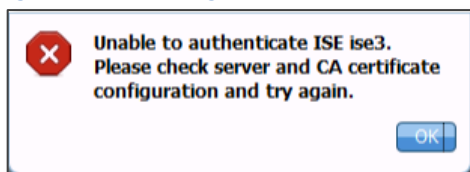
ISE clusters can only have primary and secondary administration and monitoring nodes. If you try to add another administration or monitoring node, you'll see the following error codes to warn you that your third ISE node should not be an administration or monitoring node.

Figure 19 Error Messages



Also, if your new standalone ISE node does not have a valid certificate signed by the same Root CA server that signed the primary ISE node, you'll see the following error message.

Figure 20 Error Message



After registering two or more nodes to the primary node, your list of deployment nodes should look similar to the one shown in Figure 21. Make sure that your Replication Status is COMPLETE and that Sync Status is in SYNC COMPLETED state.

Figure 21 Deployment Node Configuration Table

Deployment Nodes							
Edit Register Export Import Syncup Deregister							
<input type="checkbox"/>	Hostname	Node Type	Personas	Role(s)	Servi... ▲	Replication Status	Sync Status
<input type="checkbox"/>	ise	ISE	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	All	Not Applicable	Not Applicable
<input type="checkbox"/>	ise2	ISE	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	All	COMPLETE	SYNC COMPLETED
<input type="checkbox"/>	ise3	ISE	Policy Service		All	COMPLETE	SYNC COMPLETED

If your status is OUT-OF-SYNC, NODE NOT REACHABLE, or REPLICATION DISABLED, your primary and secondary ISE node databases are out of sync. Here are some possible causes:

- Database sync has failed because of a change in system time or an interruption during database sync.
- Nodes are not reachable.
- Certificate used to authenticate has expired.
- Secondary node has been down for more than six hours.

You may try to resolve the issue with one of the following solutions:

- For out-of-sync issues, which are usually due to time changes or Network Time Protocol (NTP) sync issues, you must correct the system time and perform a manual sync-up through the UI.
- For certificate expiry issues, you must install a valid certificate and perform a manual sync-up through the UI.
- For a node that has been down for more than six hours, you must restart the node, check for connectivity issues, and perform a manual sync-up through the UI.

Determining the Minimum Appliance Quantity and Platform

Table 2 summarizes deployment types. For centralized PSN redundancy and scaling, our recommendation assumes N + 1 load-balanced clustering.

Table 2 PSN and Endpoint Maximum Number by Deployment Model

Deployment Type	Platform	Maximum # of PSNs	Maximum # of Endpoints
Standalone Deployment (all services on same node)	All platforms	1	2,000
2-Node Redundant Deployment (all services running on each node)	All platforms	2	2,000
Administration and monitoring on the same node; policy service on dedicated node	ISE-3355	5	5,000
	ISE-3395	5	10,000
Administration and monitoring on dedicated nodes	ISE-3395	40	100,000

Table 3 lists guidelines for the maximum number of endpoints supported on each type of ISE appliance. Guidelines for VM design are to match or exceed the physical ISE appliance's specification upon which node sizing is based. Whenever a VM is used, hard disks with 10K or higher RPM are highly recommended.

Table 3 Maximum Endpoints

Form Factor	Appliance	Maximum # of Endpoints	Profiler Events
Physical	ISE-3315/1121	3,000	500/sec
	ISE-3355	6,000	500/sec
	ISE-3395	10,000	1,200/sec
Virtual	VM	10,000*	TBD

Tables 4 and 5 summarize PSN performance and posture service performance.

Table 4 Authentication Per Second

Authentication Type	Performance
PAP/ASCII	1431
EAP-MD5	600
EAP-TLS	335 (Internal) 124 (LDAP)
LEAP	445
MSCHAPv1	1064 (Local) 361 (AD)
MSCHAPv2	1316 (Local) 277 (AD)
PEAP/EAP-MSCHAPv2	181
PEAP/EAP-GTC	196 (AD) 188 (LDAP)
EAP-FAST/EAP-MSCHAPv2	192
EAP-FAST/EAP-GTC	222
Guest Logins (Web Auth) – Per PSN	10

Table 5 Posture Authentication Performance Summary

Platform	Performance
ISE 3395	110 Auth/Sec
ISE 3355	70 Auth/Sec
ISE 5515	70 Auth/Sec

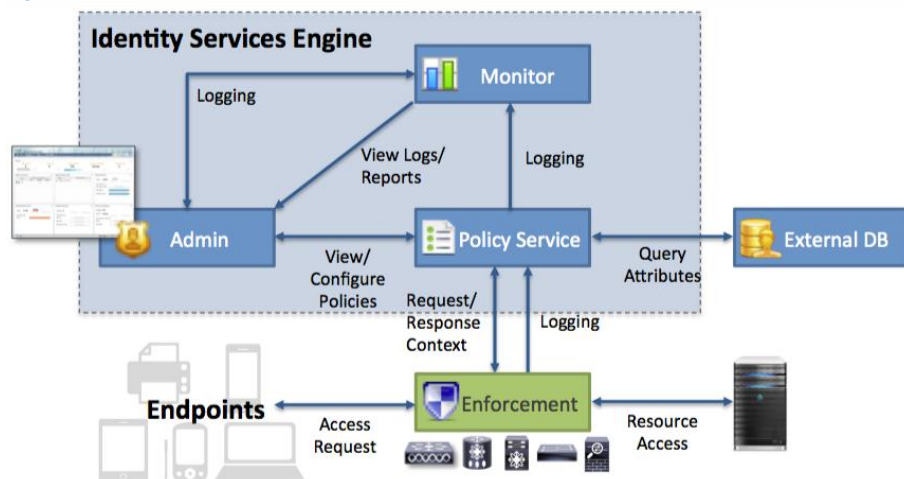
For appliance platform specifications, please refer to the following URL:

http://www.cisco.com/en/US/docs/security/ise/1.1/release_notes/ise1.1 rn.html#wp42932

Communication Between Personas

If all the personas are running on the same appliance, the appliance is used as the method for the personas to communicate. When any persona runs on a different appliance, it is important to understand how personas and appliances communicate.

Figure 22 ISE Architecture

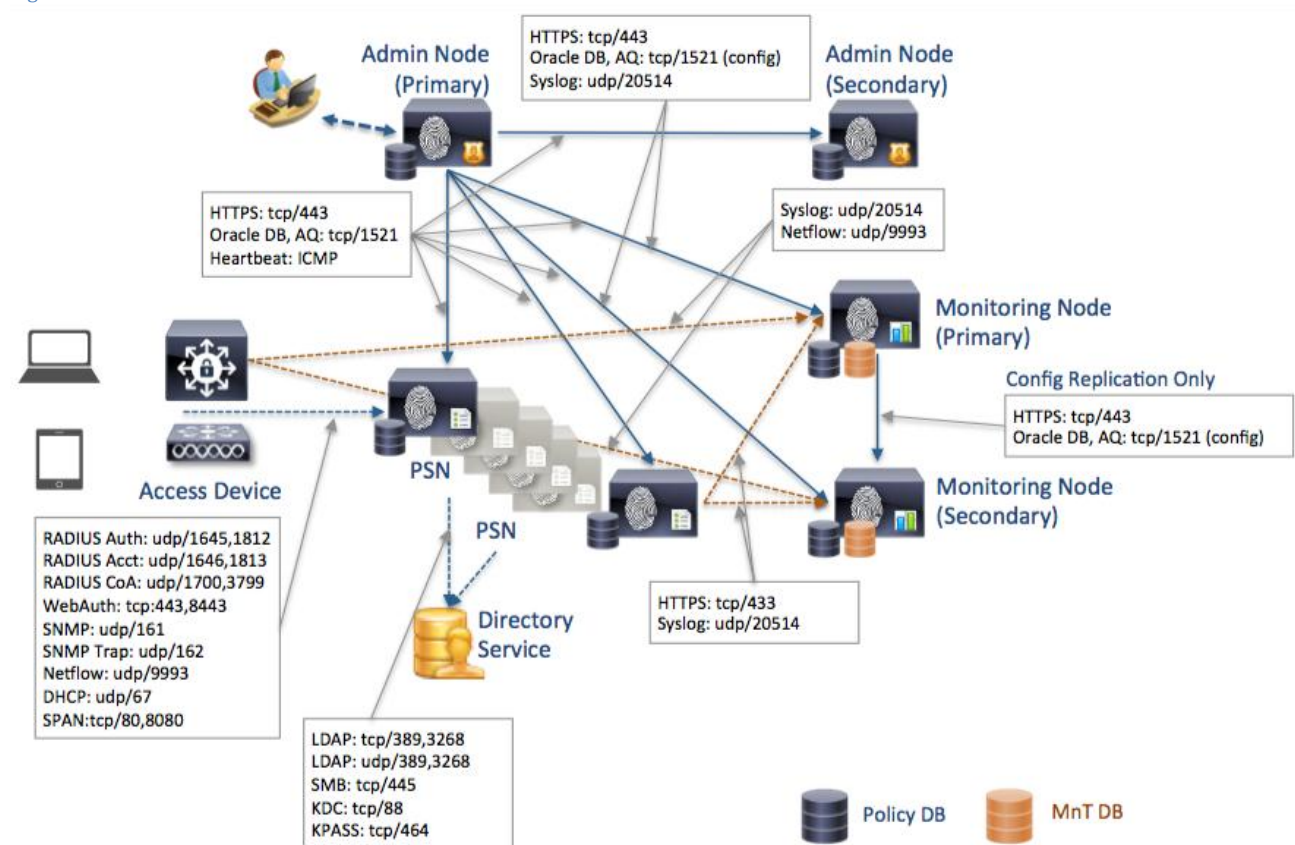


In Figure 22, all the configurations and policy changes made in the PAN are sent to the PSN. When endpoints access the network, the network access device (NAD) communicates with ISE using RADIUS. Network devices might send different types of traffic based on configured probe types (HTTP SPAN, DHCP SPAN, DHCP Relay, NetFlow, and/or SNMP Query/Trap). Those probes are targeted to specific PSN interfaces for profiling and processing. Logging information is also exchanged from all personas to the MNT.

As long as all personas are running on the same appliance, this flow happens automatically without administrator's awareness. When the personas are separated into dedicated appliances, the communications described earlier still need to happen in order to synchronize policy, collect profiling data, and store logs from other personas.

A distributed deployment design needs to support all the required communication protocols between personas. For instance, PAN and PSN communicate to replicate and synchronize policy and configurations. Those two appliances use HTTPS (TCP/443) and Oracle DB Listener and AQ (TCP/1521) to perform replication and synchronization. ICMP is also used to perform a heartbeat between the PAN and PSN. Figure 23 shows the component-level communication flow and its protocols.

Figure 23 ISE Personas and Communication Protocols



For reference, the following link provides information about Cisco ISE 3300 Series appliance ports.

http://www.cisco.com/en/US/docs/security/ise/1.1/installation_guide/ise_app_e-ports.html

Bandwidth Requirements for Distributed Deployments

As was shown in Figure 23, many types of data traverse between nodes (authentication request data and other data that is required to maintain policy). LAN speed (1 Gbps) between nodes is recommended so that there is enough bandwidth to pass data between components. If deployment involves communication on slower than LAN speed, please contact your Cisco Channel Partner or Cisco account representative for guidance.

Table 6 Bandwidth Requirement

Connection Between	Minimum Bandwidth
PAN and MNT	1 Gbps
Redundant MNT Pair	1 Gbps
PSN and PAN	1 Gbps
PSN and MNT	1 Gbps
Endpoint and PSN (Posture)	125 bps per endpoints

MNT primarily receives all logs from other components, including PAN, PSN, and NADs. Table 7 provides high-level guidance on performance.

Table 7 Monitoring Node Performance

Item	Value
Maximum syslogs (3395)	1,000/sec
Maximum sessions per day	2 million per day
Authentication per day	2 million per day
Maximum stored alarms	5,000
Reports	5,000

Appendix A: References

Cisco TrustSec System:

- <http://www.cisco.com/go/trustsec>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- For Cisco Wireless LAN Controllers:
http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html