



# Cisco TrustSec How-To Guide: Planning and Predeployment Checklists

---

For Comments, please email: [howtoguides@external.cisco.com](mailto:howtoguides@external.cisco.com)

Current Document Version: 3.0

August 27, 2012

# Table of Contents

---

Table of Contents .....	2
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
Planning Checklists .....	5
Organizational .....	5
Security Policy Creation and Maintenance.....	5
<i>Scale</i> .....	5
<i>Public Key Infrastructure (PKI)</i> .....	5
<i>Directory Services</i> .....	6
<i>Network Access Devices (NADs)</i> .....	6
<i>Managed Endpoints</i> .....	6
<i>Agentless Endpoints</i> .....	6
<i>Cisco Identity Services Engine (ISE)</i> .....	7
<i>Guest Services</i> .....	7
<i>Monitoring, Reporting, and Troubleshooting</i> .....	7
<i>Communications</i> .....	7
<i>Support Desk</i> .....	7
Deployment Checklists .....	8
Security Policy .....	8
Enforcement States.....	8
Digital Certificates.....	9
Network Services .....	9
Endpoints .....	10
Network Devices.....	10
Test Scenarios.....	11
Appendix A: References.....	12
Cisco TrustSec System:.....	12
Device Configuration Guides: .....	12

# Introduction

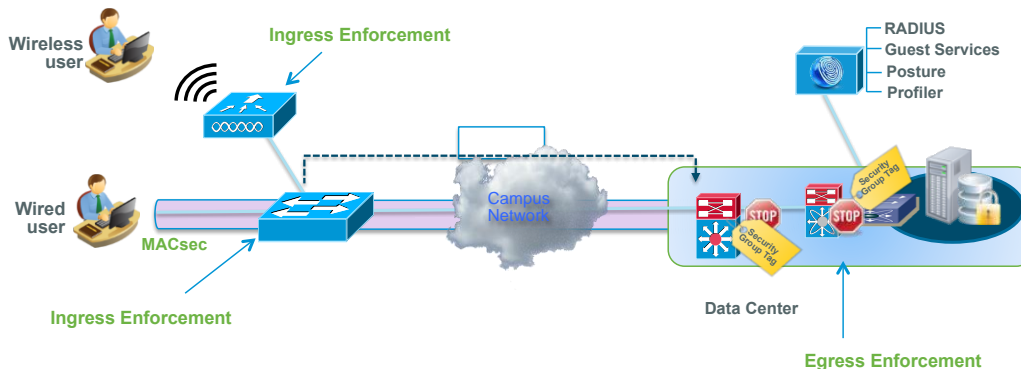
## What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. Cisco 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 Cisco 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: Cisco TrustSec Architecture Overview

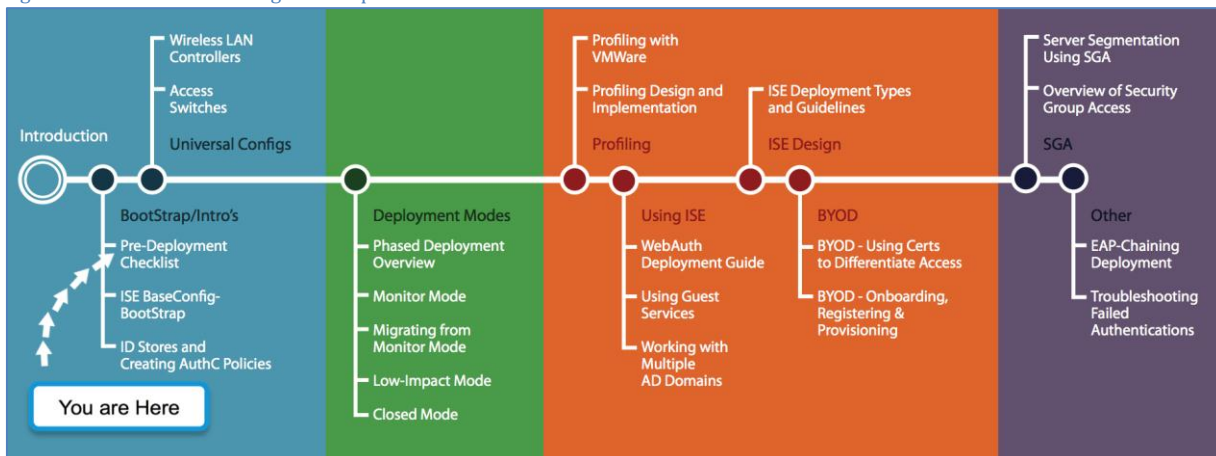


## About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for Cisco TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the Cisco 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 Cisco TrustSec deployment process (Figure 1).

Figure 2: How-To Guide Navigation Map



## What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, Cisco 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 “Cisco TrustSec “certified”. The Cisco TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the Cisco TrustSec test plans, pilot deployments, and system revisions. (i.e., Cisco 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 Cisco TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

---

# Planning Checklists

---

This checklist serves as a guide to help you understand the various components, technologies, and organizational efforts required for a successful Cisco TrustSec deployment with the Cisco® Identity Services Engine (ISE). Use this to better anticipate critical integration points so that you can verify they will work in your environment.

Answering the following organizational and operational questions will help you understand some of the security requirements, business processes, and group dynamics that will impact the integration and deployment of TrustSec in your network.

## Organizational

- Who are the organizational stakeholders required for a successful deployment and operations? For example: desktop services, network engineering, network security, domain administrators, certificate administrators, desktop support, and so on.
- Are these groups driven by a common CxO vision, or do they work independently?
- Which groups are responsible for policy creation and enforcement?
- What is the quorum of policy decision-makers for policy changes?

## Security Policy Creation and Maintenance

Please describe your desired network access policy. Include the authorization and handling of:

- Managed users including unique requirements for different groups and roles
- Unmanaged users: guests, contractors, extranets, labs, and so on
- Policies for various network access methods like wired, wireless, VPN, and virtual desktops
- Different locations: sites, buildings, floors, and so on
- Agentless devices: IP phones, printers, and so on
- Will network access authorizations be based on endpoint or user identity, endpoint posture, or both?

## Scale

- How many total locations are in your deployment?
- How many concurrent endpoints do you expect to see on the network at any time?
- How many ISE nodes will be needed? What would be the best locations within your network to place the various ISE nodes?
- Will you first test all required scenarios in a lab proof of concept (PoC) or limited production pilot?
- Will you first deploy TrustSec in your production environment in a monitor mode to gain visibility and then enforce restrictions?
- Do you have high-risk areas that you will deploy TrustSec into first?
- What is your plan to expand beyond the pilot to your entire organization?

## Public Key Infrastructure (PKI)

- Have you already deployed an enterprise PKI or certificate authority (CA)? With which vendor?

- If not, do you expect to install and manage one or purchase individual certificates from a public CA vendor?
- How much will it cost annually per server certificate?
- Each ISE node will require an individual certificate based on the full-qualified domain (FQDN) name of the node.
- What is the process for obtaining a digital certificate within your organization?
- Self-signed certificates are **not** recommended for production deployments. If you are unable to use public or enterprise CA-signed certificates, does your organization fully understand the long-term usability, support, migration, and scaling issues?

## Directory Services

- Will you use usernames and passwords or certificates to identify users and devices?
- Will you integrate with existing identity stores like Microsoft Active Directory? Lightweight Directory Access Protocol (LDAP)? RSA SecurID tokens?
- Do you have multiple identity domains or forests to authenticate against? How many?
- Will your existing identity store clusters scale to support the load from network authentication?

## Network Access Devices (NADs)

- Which edges of your network do you want to authenticate with ISE? Wired? Wireless? VPN?
- Do the relevant NADs have the software recommended for the TrustSec solution? Refer to <http://cisco.com/go/trustsec> for the latest recommended network devices and respective software versions.
- Does your existing hardware support the recommended software versions and the required TrustSec features?

## Managed Endpoints

- Do you know how many managed network endpoints are present on your network today?
- Do you already use 802.1X supplicants from Cisco or Microsoft? Wired or wireless or both?
- Will the desired 802.1X supplicant require a software purchase, upgrade, or OS service pack?
- Which authentication types are required or preferred?
- What additional security software is required for an endpoint to be compliant?
- Do you have enough security software licenses (AV, HIPS, and so on) for all required endpoints?

## Agentless Endpoints

- Do you have a method for automatically identifying and authorizing agentless endpoints on your network?
- Have you identified the total number of agentless devices and device types in your network?
  1. No 802.1X supplicant (unsupported or hardened OS such as phones or printers)
  2. Pre-Execution Environment (PXE) network booting and re-imaging
  3. Otherwise unmanaged/uncontrolled devices (guests, labs, and so on)
- What is your method of identifying, classifying, and authorizing agentless endpoints?
  1. Upgrade to 802.1X capabilities in hardware and/or OS

## 2. Whitelisting in ISE using MAC Authentication Bypass (MAB)

- What are the expected operational costs of manual MAB or endpoint registration system?

## Cisco Identity Services Engine (ISE)

- Will you need to migrate from an existing Access Control System (ACS) or Network Admission Control (NAC) appliance deployment?
- How many ISE nodes will you need to scale the deployment based on your organization size, network availability requirements, revalidation frequency, and protocol choice? Consult the TrustSec Design and Implementation Guide for how to calculate this.
- Will any load-balancing hardware or software be necessary for handling high numbers of concurrent authorizations?

## Guest Services

- What is your security policy for guests, visitors, or even employees who cannot authenticate via 802.1X or MAB?
- Will you need to migrate from an existing guest portal such as the Cisco NAC Guest Server?
- Who will be allowed to sponsor the guest accounts? Lobby staff, any employees, or self-registration?
- What are the different guest service profiles you will allow sponsors to provision? Time-of-day or time-from-first-login?
- What information will you require your guests to provide in exchange for network access?
- How will you audit sponsors, provisioned accounts, and account usage?

## Monitoring, Reporting, and Troubleshooting

- What is your existing monitoring and reporting application or toolset?
- What are your long-term storage requirements for all of these new logs and events?

## Communications

It is best to clearly communicate a change in your network access policy so noncompliant users are not surprised by new security and software requirements, access restrictions, or URL redirections.

- Do you have clear authority from management to block, limit, and redirect noncompliant endpoints and users?
- Have you raised awareness (need, benefit) for this network access change to all stakeholders and users?
- Are the responsible groups ready for a unified response to noncompliant users?
- Will these network security changes be communicated via multiple channels, including email, intranet, remediation site(s), and support desks?

## Support Desk

- Is the support staff trained for any new security technology, process, and policy?
- How will the support staff troubleshoot support calls related to ISE-based RADIUS authentications?
- Is any internal tool or application development required for ISE-related support?

# Deployment Checklists

Based on your answers to the questions in the Planning Checklist, as well as your existing network architecture, complete the following Deployment Checklist forms. These tables will be valuable references to field engineers to expedite initial configurations in Cisco ISE and network devices.

## Security Policy

Describe your major network access scenarios and how you will use contextual, network-based attributes to enforce secure access. Consider scenarios such as user versus endpoint authentication, managed endpoint posture, unmanaged endpoint identification, role-based identification and segmentation (employees, contractors, guests, and so on), or location-based differentiation. These unique authorization states will map directly to your final ISE authorization rules and policies.

Table 1: Security Policies

Scenario	User Group	Endpoint	Conditions (Location, Network Access-Wired/Wireless, Time, Authentication protocol etc.)	Authorization State
Employees using corporate devices	Domain user	Domain machine	Authentication protocol = Extensible Authentication Protocol Transport Layer Security (EAP-TLS)	Employee access
Employees using personal devices	Domain user	iPad, Android, or iPhone		

## Enforcement States

From the unique authorization states you specified in Table 1, document the specific RADIUS attribute settings for each state in Table 2. This will help you understand the subtle differences between each enforcement state and identify the number of unique ACLs you must create.

Table 2: Authorization Profiles

RADIUS Attributes	Authorization Profiles	
	Employee Access	Restricted Access
VLAN ID/Name	ACCESS	ACCESS
URL for Redirect	-	-
URL Redirect ACL	-	-
Downloadable ACL Name	ACL-ALLOW-ALL	ACL-RESTRICTED
Voice VLAN Permission	No	No
Reauthentication: Timer	28800 (8 hours)	28800
Reauthentication: Maintain Connectivity	Yes	Yes



## Digital Certificates

Create and use CA-signed certificates for your TrustSec infrastructure to minimize long-term problems due to untrusted, self-signed certificates (Table 3).

Table 3: Digital Certificates To Be Requested

Component	FQDN	Org Unit	Org	City	State	Country (2 letter)	Key Size (max)	Cert Format
Certificate Authority								
ISE Admin #1								
ISE Admin #2								
ISE PSN #1								
ISE PSN #2								

## Network Services

Document all the basic network services and the hosts that provide them in your network (Table 4). This will aid you in the creation of access control list (ACL) exceptions and TrustSec service configuration.

Table 4: List of Essential Network Services

Role	DNS Names	Network Address(es)	Protocol	Details
CA Server(s)				
DNS Server(s)			UDP:53	
DHCP Server(s)				
NTP Server(s)			UDP:123	
FTP Servers			TCP:21	username:password
Proxy Servers (to Internet)			HTTP/S:#	username:password
TFTP/PXE Boot Servers			UDP:69	username:password
Syslog Servers			UDP:514	username:password
Identity Store: Active Directory				username:password
Identity Store: LDAP				
Identity Store: OTP				
ISE Admin Node			HTTP (TCP:80) HTTPS (TCP:443)	CLI: admin: cisco Web: admin: cisco RADIUS Key:
ISE Policy Service Node			HTTP (TCP:80) HTTPS (TCP:443) RADIUS (UDP:1812) RADIUS (UDP:1813) CoA: 1700 & 3799	CLI: admin: cisco Web: admin: cisco RADIUS Key:

## Endpoints

In Table 5, specify how all the various network endpoints will be authenticated when TrustSec is enabled. Possible authentication methods include 802.1X, MAB, and web authentication.

Table 5: Endpoint Details

Endpoint	Authentication Method	Notes
Windows XP SP# (native supplicant)		
Windows Vista SP# (native supplicant)		
Windows 7 (native supplicant)		
Windows 7 (AnyConnect®)		
Windows XP SP3		
Apple Mac OS X 10.7.x (native supplicant)		
Linux		
Apple iOS devices		
Android devices		
Cisco Unified IP Phones 7900 Series		
Cisco access point		
Printers		
Servers		
Guests		
PXE Boot		

## Network Devices

Use Table 6 to document each type of network access device in your network by model, supervisor (if appropriate), and software version. It is highly recommended that you upgrade all switches to the latest tested and validated TrustSec version to avoid feature and behavioral inconsistencies. Each network device IP address must be added to ISE unless you use wildcard entries.

Table 6: Network Device list

Model	Cisco IOS® Software Version	Management IP Address	Management DNS Name

## Test Scenarios

Based on your desired security policy, anticipated endpoints, and enforcement states, create a list of scenarios to test in your lab or small proof of concept deployment before deploying at scale. Table 7 lists some suggested scenarios to get you started.

Table 7: Test Scenarios

Scenario	Result (Pass/ Fail)	Comments
Device Profiling		
MAB		
Windows Machine Authentication		
User Authentication to Active Directory Domain		
Single Sign-On (SSO): Username/Password		
Guest Sponsorship		
Guest Access		

# 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](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](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](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](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](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](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](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](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](http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html)