**[ISE Planning & Pre-Deployment Checklists](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635)**

edited ‎02-21-2020 10:02 PM

* [How to Use These Checklists](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--1994416716)
* [Planning Checklists](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-493096117)
* [Business Objectives](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1183657591)
* [Organizational](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--623796872)
* [Security Policy Creation and Maintenance](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1863715961)
* [Scale](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-56261498)
* [Public Key Infrastructure (PKI)](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--1751192965)
* [Directory Services](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-736319868)
* [Network Access Devices (NADs)](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--1071134595)
* [Managed Endpoints](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1416378238)
* [Assets](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1282693514)
* [Cisco Identity Services Engine (ISE)](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--524760949)
* [Guest Services](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1962751884)
* [Monitoring, Reporting, and Troubleshooting](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-155297421)
* [Communications](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--1652157042)
* [Support Desk](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-835355791)
* [Deployment Checklists](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1386331442)
* [Network Services](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--292040302)
* [Digital Certificates](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--2099494765)
* [Network Devices](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1086180009)
* [Security Policy](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--721274454)
* [Enforcement States](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId-1766238379)
* [Endpoints](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--41216084)
* [Test Scenarios](https://community.cisco.com/t5/security-knowledge-base/ise-planning-amp-pre-deployment-checklists/ta-p/3622635#toc-hId--1848670547)

**How to Use These Checklists**

These checklists serve as guides to help you understand the various requirements, components, technologies, and organizational efforts required for a successful design and deployment of the Cisco Identity Services Engine (ISE). 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 segmentation in your network.

For an offline/printed copy of this document, simply choose **Options > Printer Friendly Page**. You may then Print or Print to PDF or copy and paste to Word or any other document format you like.

**Planning Checklists**

**Business Objectives**

Ultimately, all security policies directly reflect the business' need to minimize the risks and threats to daily business operations and brand. Many of these are preventative measures and some may required by regulations. Identifying these business-critical needs can help you to quickly establish your priorities and policies for Who, What, and Where your network is secured.

* What laws or regulations subject your business to audits that are impacted by network security?
* Have you recently had network security incidents that impacted your business operations affected brand reputation?
* What keeps your chief information security officer awake at night?
* What and where are your most critical assets that need protection on the network?
* What do you feel are the weakest links in your network security today?

**Organizational**

After establishing the your business objectives for network security, you will need to understand everyone involved for implementation. While the underlying protocols and mechanisms that ISE uses to control access to the network work at Layers 2 & 3, you would be surprised how many deployment difficulties occur at "Layer 8". This is due to how ISE unifies access across wired, wireless and VPN networks and performs asset visibility, compliance and threat control requiring the collaboration of many network and IT departments.

* 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 different departments or teams required to configure and maintain different parts of the access control system from the endpoints and agents to network devices to policy enforcement to user or asset databases to security applications?
* Are these groups driven by a common CxO vision, or do they work independently?
* Which group(s) 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 existing and desired network access policies. 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?
* What technologies will you use for enforcing network access controls: VLANs, ACLs, or software-defined segmentation?

**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 monitor and identity users and endpoints to gain visibility and capability or configuration information before applying enforcement?
* Do you have high-risk areas that you will enforce 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?

**Assets**

* Do you have a method for automatically identifying and authorizing agentless endpoints on your network? MAC Authentication Bypass (MAB) or 802.1X or endpoint profiling?
* Have you identified the total number of agentless devices and device types in your network?
* What is your method of identifying, classifying, and authorizing agentless endpoints?
* 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 above, 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.

**Network Services**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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: |

**Digital Certificates**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 Devices**

Use the Network Devices List 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 validated software version in the [ISE Compatibility Guides](http://cs.co/ise-compatibility) and [TrustSec Platform Support Matrix](http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html) to avoid feature and behavioral inconsistencies.  Each network device IP address must be added to ISE unless you use wildcard entries.

|  |  |  |  |
| --- | --- | --- | --- |
| **Model** | **Cisco IOS® Software Version** | **Management IP Address** | **Management DNS Name** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**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. Below are some pseudo-policy examples.

|  |  |  |
| --- | --- | --- |
| **Scenario Name** | **Conditions (Who, What, When, Where, How)** | **Authorization**  **Result** |
| Corporate Workstation | Active Directory Domain Computers | Workstation\_Access |
| Phones | Profiled IP Phones | Voice\_Network |
| Printers | Profiled Printers | Printer\_Network |
| Employee | AD Employees | Employee\_Access |
| BYOD | AD Employees & Registered Device | Internet\_Only |
| Guest | Guest SSID & Sponsored Guest | Internet\_Only |
| Default | - | Guest\_Redirect |

**Enforcement States**

Identify the specific RADIUS authorization attributes for each unique authorization states you identified in your Authorization Poliicy. This will help you understand the subtle differences between each enforcement state and identify the number of unique ACLs or Scaleable Group Tags that you must create.

|  |  |
| --- | --- |
| **RADIUS Attributes** | **Authorization Profiles** |
| Workstation\_Access | VLAN: Data  dACL: ACL-WORKSTATIONS  Session Timeout: 86400 (24 hours) |
| Voice\_Network | Voice VLAN Permission: Yes  Session Timeout: 86400 (24 hours) |
| Printer\_Network | VLAN: Data  dACL: ACL-PRINT-SERVERS  Session Timeout: 86400 (24 hours) |
| Employee\_Access | VLAN: Data  dACL: ACL-EMPLOYEE-ACCESS  Session Timeout: 28800 (8 hours) |
| Internet\_Only | VLAN: Data  dACL: ACL-INTERNET-ONLY  Session Timeout: 28800 (8 hours) |
| Guest\_Redirect | URL-Redirect: ACL-CENTRAL-WEBAUTH  URL-Redirect-ACL: ACL-URL-GUEST-REDIRECT  Session Timeout: 600 (10 minutes) |

**Endpoints**

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

|  |  |  |
| --- | --- | --- |
| **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 IP Phones |  |  |
| Cisco Access Point |  |  |
| Printers |  |  |
| Guests |  |  |
| PXE Boot |  |  |

**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.

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Result (Pass/ Fail)** | **Comments** |
| MAB |  |  |
| Phone |  |  |
| Printer |  |  |
| Other |  |  |
| IOT: Camera |  |  |
|  |  |  |
| MAB+Profiling |  |  |
| User Authentication to Active Directory Domain |  |  |
| Single Sign-On (SSO): Username/Password |  |  |
|  |  |  |
| Windows Machine Authentication (Wired) |  |  |
| 802.1X Windows Native Supplicant Machine Authentication using PEAP-MSCHAPv2 |  |  |
| 802.1X Windows Native Supplicant Machine Authentication using EAP-TLS |  |  |
| 802.1X Windows Native Supplicant Machine Authentication on Docking Station |  |  |
| 802.1X Windows Native Supplicant Machine Authentication behind IP Phone |  |  |
| 802.1X Windows Native Supplicant Machine Authentication in VM on PC in Docking Station behind IP Phone |  |  |
| 802.1X Windows Native Supplicant Machine Authentication after Sleep/Hibernation |  |  |
|  |  |  |
| Windows User Authentication (Wired) |  |  |
| 802.1X Windows Native Supplicant Username+Password (PEAP-MSCHAPv2) |  |  |
| 802.1X Windows Native Supplicant User Certificate (EAP-TLS) |  |  |
| 802.1X Windows Native Supplicant User Authentication: Not domain-joined |  |  |
| 802.1X Windows Native Supplicant User Authentication: Domain-joined |  |  |
| 802.1X Windows Native Supplicant User Authentication on Docking Station |  |  |
| 802.1X Windows Native Supplicant User Authentication behind IP Phone |  |  |
| 802.1X Windows Native Supplicant User Authentication in VM on PC in Docking Station behind IP Phone |  |  |
| 802.1X Windows Native Machine Authentication after Sleep/Hibernation |  |  |
| Remote Desktop Protocol (RDP) Login with Windows Native Supplicant |  |  |
|  |  |  |
| Windows with AnyConnect (Wired and/or Wireless) |  |  |
| 802.1X AnyConnect NAM using PEAP-MSCHAPv2 |  |  |
| 802.1X AnyConnect NAM using EAP-TLS |  |  |
| 802.1X AnyConnect NAM EAP Chaining Machine (EAP-FAST: Certificate) |  |  |
| 802.1X AnyConnect NAM EAP Chaining User (EAP-FAST: Username) |  |  |
| 802.1X AnyConnect NAM EAP Chaining Both (EAP-FAST: Machine Certificate + Username) |  |  |
|  |  |  |
| Easy Connect |  |  |
| 802.1X + Passive-ID - Post |  |  |
| 802.1X + Passive-ID - Post |  |  |
| Easy Connect - Post |  |  |
|  |  |  |
| Wireless |  |  |
| 802.1X iOS |  |  |
| 802.1X Android |  |  |
| 802.1X Other Mobile OS |  |  |
| 802.1X BYOD post-onboarding using EAP-TLS |  |  |
| 802.1X Anonymous |  |  |
|  |  |  |
| Guest Access (Wired and/or Wireless) |  |  |
| Guest: Hotspot (with/out Passcode, AUP, etc.) |  |  |
| Guest: Registration & Login |  |  |
| Guest: Sponsor User Creation |  |  |
| Guest: Sponsored User Login |  |  |
| WebAuth: Employee login with AD |  |  |
| CWA Chaining (Cert) Initial WebAuth pending |  |  |
| CWA Chaining (Cert) |  |  |
| CWA Chaining (Username) WebAuth pending |  |  |
| CWA Chaining (Username) |  |  |
|  |  |  |
| Posture |  |  |
| EAP Chaining Both (Machine cert + username) Posture pending |  |  |
| EAP Chaining Both (Machine cert + username) Posture compliant |  |  |
|  |  |  |
| VPN |  |  |
| AnyConnect SSL VPN Username+Password |  |  |
| AnyConnect SSL VPN Certificate |  |  |
|  |  |  |