**[ISE High Level Design (HLD)](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418)**

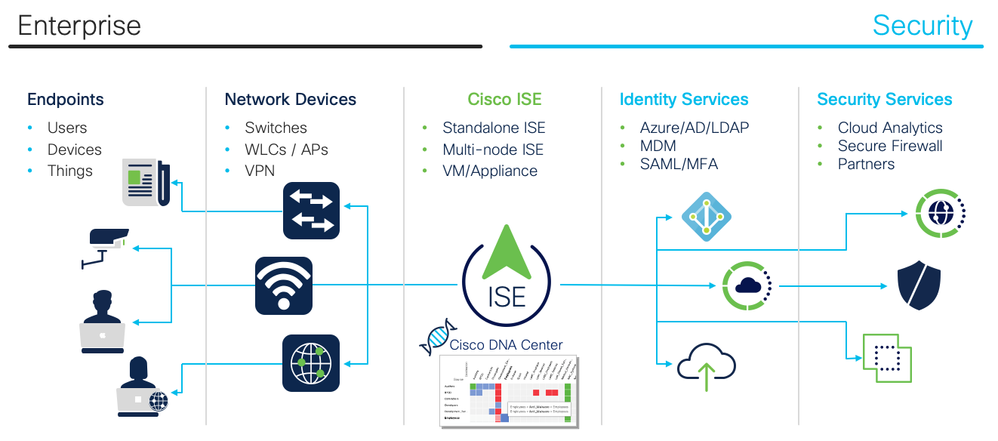
[thomas](https://community.cisco.com/t5/user/viewprofilepage/user-id/26555)

Contents

* [Instructions](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-506516758)
* [Introduction](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1300937705)
* [Business Objectives](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1186575128)
* [Environment](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--620879335)
* [Network Architecture Diagram](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-69682139)
* [Trust & Identity Services](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1737772324)
* [User Groups](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-749740509)
* [Network Devices](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1057713954)
* [Endpoints](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1429798879)
* [ISE Architecture](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--377655584)
  + [Scenarios](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1285611051)
* [Device Administration (TACACS+)](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--392760693)
* [Visibility](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-2094752140)
* [Secure Wireless](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-287297677)
* [Guest](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1520156786)
* [HotSpot](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-967356047)
* [Self-Registered](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--840098416)
* [Sponsored](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1647414417)
* [API](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--160040046)
* [BYOD](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1967494509)
* [Secure Wired](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1218180265)
* [VPN](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--589274198)
* [Compliance & Posture](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1898238635)
* [Segmentation](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-90784172)
* [Security Integrations](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1716670291)
* [Context Exchange](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-770842542)
* [Rapid Threat Containment (RTC)](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--1036611921)
* [Threat-Centric NAC](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-1450900912)
* [REST APIs](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--356553551)
* [Operations & Management](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-2001876563)
* [Scale & High Availability](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId-892584041)
* [Policy Details](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--914870422)
* [Resources](https://community.cisco.com/t5/security-knowledge-base/ise-high-level-design-hld/ta-p/3657418#toc-hId--2042266515)

**Introduction**

An ISE High Level Design (HLD) is recommended to assist you with the design and planning of your ISE deployment. Having a clearly written security policy - whether aspirational or active - is the first step in assessing, planning and deploying network access security.  Without this, it is hard to break down the deployment into phases by location or capabilities. When seeking outside help, the HLD provides a huge time savings for education other teams, partners, Cisco Sales representative, Technical Assistance Center (TAC) representative or even the ISE product and engineering teams. Clearly state the desired solution capabilities, hardware and software environment and integrations can quickly allow people to understand what you want and how to configure it or troubleshoot it.



**Business Objectives**

Identify the Customer Business Objectives that ISE must solve. Typically this involves regulations and compliance or identified security threats and risks to smooth operation of the business or brand. But it also involves mitigating risks with controlled network access for everyday IT processes. This is how you begin to craft your network access control policy. The more specific you can be, the better.

Consider the following example business objectives that must translate into access control policy :

* We want to provide sponsored guest access to our visitors
* All network device administration commands must be authorized and logged for potential audit
* We want to identify all endpoints on our network so we can begin to apply access control policies
* We do not want our employees personal devices on our corporate network
* We want our employees to any device they want but we want to manage it to ensure it and any information on it is properly secured
* Printers should only talk to print servers
* We need to be able to re-image our workstations over the network via PXE
* We must comply with [PCI, HIPAA, etc.] regulation
* All Windows devices must be patched within the last 30 days to minimize known vulnerabilities
* We want to automatically quarantine endpoints when [Stealthwatch, AMP, etc.] detects malicious behavior

|  |
| --- |
| Business Objectives |
|  |

**Environment**

|  |
| --- |
| **Network Architecture Diagram** |
| <Insert image of your network architecture with ISE here> |

**Trust & Identity Services**

List all of the products that ISE will need to integrate with for authoritative trust and identity for authentication and authorization. Please note any known issues or concerns with their behavior, capabilities or scale.

Note: Cisco strongly recommends server certificate, which is signed by in-house CA or other 3rd party Root CA server, to be used for ISE. Self-signed server certificate should *not* be used for production deployment.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario (one line per device to be validated) | Vendor / Version | Count | Notes |
| **Identity Sources** |  |  |  |
| **Certificate Authorities (CA)**   * How will ISE integrate with 3rd party CA? * Will ISE be issuing certificates for BYOD? * Utilize web based CA portal on ISE? * Utilize API for certificate management? * Utilize AnyConnect/ASA for SCEP enrollment? |  |  |  |
| **Active Directory**:   * How many AD domains / forests are to be integrated? * ISE requires AD forest DNS consolidated into central DNS servers. What method is used to consolidate DNS information for the separate AD forests? * What version of AD is in use? * Are there any Read-Only domains in place? * AD Site & Services is recommended for ISE in all forests. | Microsoft | # |  |
| LDAP |  | # |  |
| Token |  | # |  |
| SAML |  | # |  |
| ODBC |  | # |  |
| Social Login | Facebook? | # |  |

**User Groups**

Identify the specific user groups that will require differentiated access and for which scenarios.

|  |  |
| --- | --- |
| Scenario (one line per device to be validated) | Notes |
| **Groups** |  |
|  |  |
|  |  |

**Network Devices**

Provide the general switch/controller model numbers/platforms deployed and Cisco IOS and AireOS Software versions to be deployed to support ISE design. Please use the [ISE Compatibility Guides](http://cs.co/ise-compatibility) to see our latest list of Validated products and protocols. If you still don't believe that ISE supports heterogeneous networks and can support your network devices, please read [Does ISE Support My Network Access Device?](https://community.cisco.com/docs/DOC-75329)

|  |  |  |  |
| --- | --- | --- | --- |
| Vendor | Hardware Model @ Software Version | Count | Notes |
| **Wired** |  |  |  |
| Cisco | 9300 @ IOS-XE 15.x.x | # |  |
| **Wireless** |  |  |  |
| Cisco | WLC xxxx @ AireOS 8.x | # |  |
| Cisco | Meraki xxxx |  |  |
| **VPN** |  |  |  |
| Cisco | ASA 55xx @ x.x | # |  |

**Endpoints**

List all of the unique endpoint types you expect to find and apply policy to in your deployment.

Provide an approximate number of each of possible.

Note: For domain joined Windows machines to function properly, machine authentication is recommended. Performing user only authentication may break critical functions such as machine GPO and other background services such as backup and software push.

Note: State whether the deployment is using machine or user authentication, or both. If both machine and user authentication are planned, are Machine Access Restrictions (MAR) planned? If so, review the Appendix information on MAR caveats. For machine / user authentication details, please refer to [802.1X Authenticated Wired and Wireless Access](http://technet.microsoft.com/en-us/library/cc730878%28WS.10%29.aspx)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Endpoints (one line per scenario to be validated) | Vendor | Hardware Model @ Software Version | Count | Notes |
| **Workstations** |  |  |  |  |
| WindowsXP | Microsoft | Windows XP | # |  |
| Windows7 | Microsoft | Windows 7.x | # |  |
| Windows8 | Microsoft | Windows 8.x | # |  |
| Windows10 | Microsoft | Windows 10 | # |  |
| Kiosk | Microsoft | Windows Embedded | # |  |
| MacBook | Apple | macOS 11.2 | # |  |
| MacBook | Apple | macOS 10.15 | # |  |
| Chromebook |  |  | # |  |
| Linux |  | Linux | # |  |
| VDI |  |  |  |  |
| **Mobile Devices** |  |  |  |  |
|  | Apple | iOS 14.x |  |  |
|  | Apple | iOS 13.x |  |  |
|  | Apple | iOS 12.x |  |  |
|  | Android | Android 11.x |  |  |
|  | Android | Android 10.x |  |  |
|  | Android | Android 9.x |  |  |
| **Office** |  |  |  |  |
| Access Points | Cisco |  | # |  |
| IP Phones | Cisco | 7xxx | # |  |
| Printers |  |  | # |  |
| **IOT** |  |  |  |  |
| Cameras |  |  | # |  |
| Lighting |  |  | # |  |
| Badging |  |  | # |  |
| HVAC |  |  | # |  |
| Medical |  |  | # |  |
| Manufacturing |  |  | # |  |
| SCADA |  |  | # |  |
| Others |  |  | # |  |
|  |  | **Approximate Total:** | **###** |  |

**ISE Architecture**

List all of the nodes in your ISE deployment.

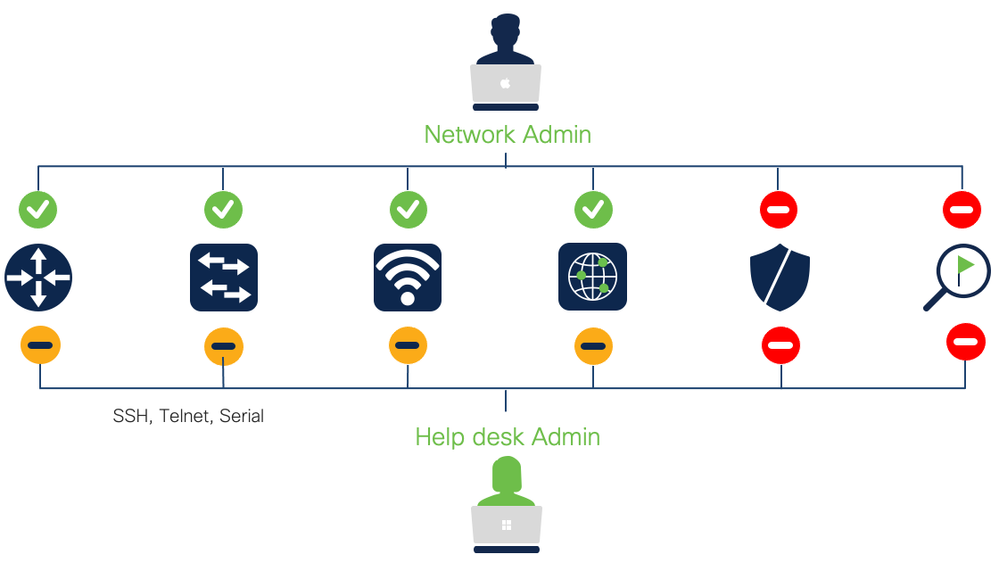
When deploying VMs:

* The VM host should be sized comparably with the ISE hardware appliance(s)
* The phyiscal RAM and CPU resources *must be reserved* for each ISE node and *cannot be shared* among different ISE nodes or other guest VMs on the VM host. If you cannot do this, please use physical appliances.
* Hard disks with 10K or higher RPM are required. Average IO Write performance for the disk should be higher than 300MB/sec and IO Write performance should be higher than 50MB/sec.
* For the MnT nodes, it is highly recommended to use SSD/Flash storage to greatly improve read/write performance

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Host Name (FQDN)** | **Persona** | **IP Address** | **VM/HW** | **Size** | **Storage** |
| ise1.example.com | PAN+MnT |  | VM | 3695 | 600GB |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Scenarios**

**Device Administration (TACACS+)**



Differentiated access for network device administrators

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| SuperAdmin |  |  |
| NetworkAdmin |  |  |
| HelpDesk |  |  |
| AutomationScript |  |  |
| ReadOnlyAdmin |  |  |

**Visibility**

See what, when, where and how users and endpoints are on your network.

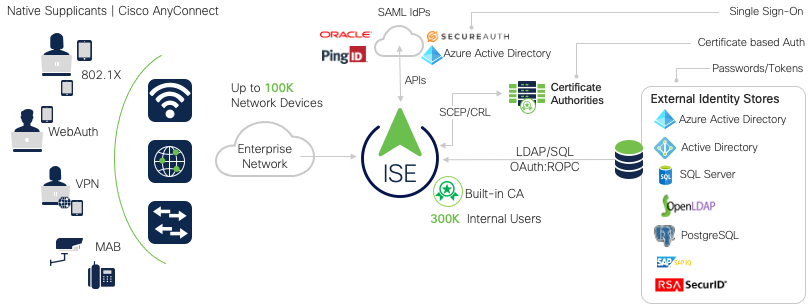
In the table below, list the primary endpoint devices (one per row) that need to be profiled.

* Identify the primary device types to be profiled
* Which probes/protocols will be used to collect the required data? Leverage Device Sensor to collect endpoint attributes whenever possible and SNMP for other network devices. Uncommon devices may require collecting additional protocol attributes to classify the endpoint properly.
  + ISE Probes: AD, DHCP, DNS, HTTP, NMAP, RADIUS, SNMP, Netflow
  + Device Sensor: CDP, LLDP, DHCP, HTTP, H323, SIP, MDNS
  + AnyConnect: ACIDex
* What is the endpoint attribute data required to classify each device type?
* Is profiling for visibility only or for use in authorization policy?
* Leverage Device Sensor to collect endpoint attributes whenever possible and SNMP for other network devices
* Uncommon devices may require collecting additional protocol attributes to classify the endpoint properly.
* For Visibility with SPAN/RSPAN, use a dedicated interface on the ISE PSN for the DHCP SPAN or HTTP SPAN probe.
* If RSPAN or Netflow is to be used:
  + does infrastructure support these technologies?
  + a dedicated interface should be used on the Policy Service Node for the DHCP SPAN or HTTP SPAN probe. Is there sufficient bandwidth between source SPAN/Netflow exporter and ISE Policy Service node used for profiling?

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| Enable Profiling Feed Service or retrieve offline update |  |  |
| Create Custom Endpoint Profiles for \_\_\_\_\_ Devices |  |  |
| Create Endpoint Purge Policies |  |  |
| Move profiled endpoints to static MAC-based endpoint lists and do not use endpoint profiles in authorization rules if you want to minimize Plus License consumption |  |  |
|  |  |  |
|  |  |  |

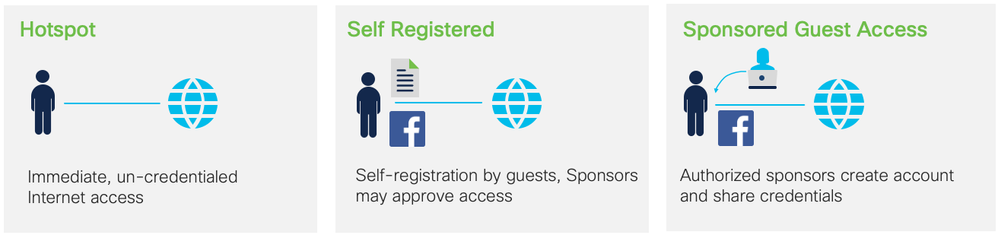
**Secure Wireless**

Control authenticated endpoint & user access



|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Wireless** |  |  |
| Wireless 802.1X User Authentication & Authorization: Show Successful Login and Role-Based Access |  |  |
| Wireless Machine Authentication and Authorization: use digital certificate for Corporate device |  |  |
| Individual Pre-Shared Key (iPSK) |  |  |
| Static Endpoint MAC Whitelisting: allow non-authenticating (no 802.1X) endpoints with MAB |  |  |
| Wireless user with Passive Identity (No 802.1x) |  |  |
| [eduroam](https://community.cisco.com/docs/DOC-75525) |  |  |
|  |  |  |

**Guest**



Internet access for visitors. Generally, you should only implement one type of Guest network.

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **HotSpot** |  |  |
| Customize Portal   * Behavior: Acceptable Usage Policy (AUP), Password, Auto-Login, Success URL, etc. * Presentation: Logo, Colors, Fonts |  |  |
| Demonstrate Hotspot with desired flow: |  |  |
| **Self-Registered** |  |  |
| Create desired Guest Types |  |  |
| Demonstrate Self-Service Guest registration |  |  |
| **Sponsored** |  |  |
| Customize Sponsor Portal Flow and Presentation |  |  |
| Create Sponsor Groups |  |  |
| Demonstrate Sponsor Portal (sponsored Guest access) |  |  |
| Login with Sponsored Guest Credentials |  |  |
| Concurrent Guest Logins |  |  |
| **API** |  |  |
| Guest API integration with external application(s) |  |  |

**BYOD**

Onboard & differentiate personal & corporate devices. Consider the following topics when determining your scenarios:

* Is it Single SSID or Dual SSID?
* Will Android be in the BYOD design? If so, please provide details of provisioning authorization profile
* What devices will and will not be  provisioned?
* What supplicant will be used? Native or AnyConnect or Other?
* What access will unsupported device get? (i.e. Blackberry, Windows phones, Chromebooks)
* Will EMM/MDM be integrated with BYOD design? If so, please provide details of MDM policy below in the Authorization Policy section and whether or not redirection will be used for MDM agent installation

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Device Registration** |  |  |
| Single SSID: Unregistered devices are redirected to a WebAuth portal and respective users |  |  |
| Dual SSID: Unregistered devices are redirected to a WebAuth portal and respective users |  |  |
| **Certificate Provisioning** |  |  |
| BYOD: Onboarding, Certificate Provisioning with Internal or External CA |  |  |
| Certificate Expiration with Internal or External CA |  |  |
| Certificate Renewal 2-4 weeks before Certificate Expiration |  |  |
| **Device Management** |  |  |
| Certificate Revocation by Administrator |  |  |
| End-User self management, Device Lost; Blacklist endpoint |  |  |
| End-User self management, Device Stolen; revoke Certificate |  |  |

**Secure Wired**

Control authenticated endpoint & user access

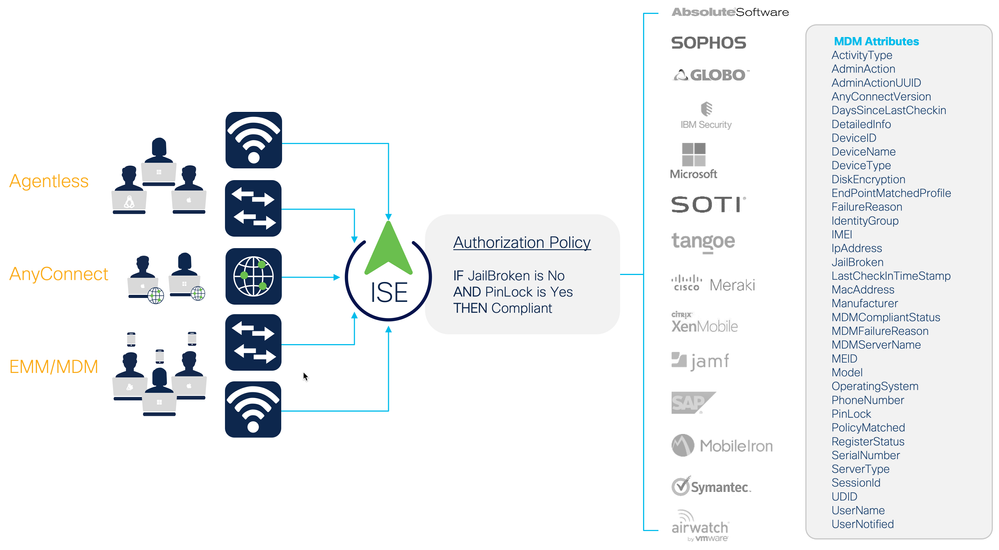
|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Wired** |  |  |
| [ISE Wired Access Deployment Guide](https://community.cisco.com/t5/security-documents/cisco-ise-wired-access-deployment-guide/ta-p/3641515) |  |  |
| [Static Endpoint MAC Whitelisting](https://community.cisco.com/docs/DOC-76521): allow non-authenticating (no 802.1X) endpoints with MAB |  |  |
| [Static Endpoint MAC Blacklisting](https://community.cisco.com/docs/DOC-76521): block non-authenticating endpoints with MAB |  |  |
| Dynamic Endpoint Profiling and Authorization: *List each endpoint profile and the desired authorization* |  |  |
| Easy Connect: Wired user with Passive Identity (No 802.1X supplicant) |  |  |
| Wired Web Authentication (No 802.1X Supplicant. For Guest or Employees) |  |  |
| EAP-Chaining: Wired machine+user authentication using EAP-FAST with AnyConnect |  |  |
| Wired Machine Authentication and Authorization: use digital certificate for Corporate device |  |  |
| Wired User 802.1X Authentication: Show Successful Login and Role-Based Access |  |  |
| Wired WebAuth Login: Show Login With No Supplicant |  |  |
| Wired Authentication (user or machine) & Authorization on a Docking Station |  |  |
| Wired Authentication for a user via an Windows Remote Desktop Protocol (RDP) Session |  |  |
| Wired Authentication for Multi-User devices (Nurses Station, Call Center, etc.) |  |  |
| Wired Authentication (user or machine) & Authorization on a Docking Station Behind IP-Phone |  |  |
| Wired Authentication with Two-Factor Authentication (2FA) |  |  |
|  |  |  |

**VPN**

Control remote access of endpoints and users.

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **VPN** |  |  |
| VPN Authentication and Authorization with Username:Password: Show Successful Login and Role-Based Access |  |  |
| VPN Authentication and Authorization with Token/2FA: Show Successful Login and Role-Based Access |  |  |
| VPN Access Attempt, Revoked Certificate (Testing OCSP) |  |  |

**Compliance & Posture**



Ensure that endpoints meet security standards.

Review the list of currently supported packages for [Windows](http://www.cisco.com/c/dam/en/us/td/docs/security/ise/1-2/release_notes/win-avas-3_5_6317_2.pdf) and [macOS.](http://www.cisco.com/c/dam/en/us/td/docs/security/ise/1-2/release_notes/mac-avas-3_5_6317_2.pdf)

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Agent-less** |  |  |
| Posture Windows with Temporal Agent |  |  |
| Posture macOS with Temporal Agent |  |  |
| **Agent-ed** |  |  |
| Non-Compliant endpoints are quarantined and redirected to provision AnyConnect and the Posture Module via ISE |  |  |
| Non-Compliant endpoints are quarantined and redirected until provisioned by [WSUS, etc.] |  |  |
| Compliant endpoints are properly authorized on the network |  |  |
| **Enterprise Mobility Management (EMM) / Mobile Device Management (MDM)** |  |  |
| Integrate ISE with EMM/MDM vendor(s) |  |  |
| Non-Compliant endpoints are quarantined and redirected until provisioned by [WSUS, etc.] |  |  |
| Compliant endpoints are properly authorized on the network |  |  |

**Posture Policies**

Describe posture policy requirements for endpoint compliance. This may include many areas such as asset checking, application and services checking, and antivirus and antispyware checks, as well as customized checks for specific use cases. Describe remediation plans and include remediation servers that need to be integrated into the design.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rule Name** | **OS (Windows/macOS)** | **Conditions** | **Posture Agent** | **Checks** | **Remediation** | **Enforcement (Audit/Opt/ Mandatory)** | **When Assessed (Login/PRA/Both)** |
| Employee\_AV | Windows XP/7 | AD group= Employee | NAC Agent for Windows | AV Rule: Microsoft Security Essentials 2.x | Live update (Automatic) | Mandatory | Both |
| Employee\_Asset | Windows XP/7 | AD group= Employee | NAC Agent for Windows | Custom registry check | Link redirect to policy page (Manual) | Mandatory | Login |
| Contractor\_AV | Windows ALL | ID Group= Contractor | Web Agent | AV\_Rule: Any AV w/current signatures | Local Message regarding AV Policy | Mandatory | Login |

**Client Provisioning Policies**

Describe Client Provisioning policy requirements for posture and native supplicant provisioning.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rule Name** | **Identity Groups** | **Operating Systems** | **Other Conditions** | **Results** |
| Apple | Any | MAC OSX or Apple iOS |  | **Native Supplicant:**  EAP-TLS, SSID |
| Windows | Any | Windows All |  | **Agent:** NAC Agent  **Native Supplicant:**  PEAP-MSCHAPv2, SSID |
| Android | Any | Android |  | **Native Supplicant:**  EAP-TLS, SSID |

**Segmentation**

Limit exposure with pre-defined access segmentation.

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Classification** |  |  |
| Dynamically classify endpoints with SGTs via MAB (static or profiled, e.g. IOT) |  |  |
| Dynamically classify endpoints with SGTs via 802.1X Machine Authentication |  |  |
| Dynamically classify users with SGTs via 802.1X Authentication |  |  |
| Dynamically classify users with SGTs via Easy Connect (MAB+Passive Identity) |  |  |
| Dynamically classify users with SGTs using WebAuth (e.g. Guests) |  |  |
| Statically classify traffic by VLAN |  |  |
| Statically classify traffic by Subnet |  |  |
| Statically classify traffic by L2 Interface |  |  |
| Statically classify traffic by L3 Port |  |  |
| Statically classify traffic by VM (port profile) |  |  |
| **East-West Segmentation** |  |  |
| Malware blocking between Employees |  |  |
| Virtual machines in the data center |  |  |
| **Firewall Rule Reduction** |  |  |
| Use group-based policies to reduce firewall rules by eliminating need to specify IPv4/IPv6 addresses |  |  |
| **User to Data Center** |  |  |
| Use group-based policy to enforce access to resources in the data center |  |  |

**Security Integrations**

Share contextual information with other products using Cisco Platform Exchange Grid (pxGrid) and REST APIs.

See the full list of technology partners at [Cisco Security Technology Alliance](https://www.cisco.com/go/csta).

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Context Exchange**  Sharing network identity (Who/What/When/Where/How) with other network and security services. |  |  |
| Cisco Firepower |  |  |
| Cisco Stealthwatch |  |  |
| Cisco Web Services Appliance (WSA) |  |  |
| SIEM (Splunk) |  |  |
| Cisco Industrial Network Director (share IOTAsset topic with ISE) |  |  |
| ... |  |  |
| **Rapid Threat Containment (RTC)**  Security services with their own policy that tell ISE when to deny/quarantine a specific user or device. |  |  |
| Stealthwatch |  |  |
| ... |  |  |
| **Threat-Centric NAC**  Security services provide CVSS threat and vulnerability information to ISE for deny/quarantine decisions. |  |  |
| Vulnerability Scanner |  |  |
| AMP |  |  |
| ... |  |  |
| **REST APIs** |  |  |
| Integrate Guest Management workflow from another application |  |  |
| Integrate DNA Center with ISE for Access Control Policy and software-defined Segmentation with TrustSec |  |  |
| Integrate network management tool for adding/updating/removing network devices, endpoints, etc. |  |  |
| ... |  |  |

**Operations & Management**

List the day-to-day operations you anticipate needing to do.

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **Monitoring** |  |  |
| Real-Time Event Log (Live Log) |  |  |
| Illustrate the Live Log Authentication Details |  |  |
| Debug Endpoint (Working across entire ISE deployment) |  |  |
| TCP Dump from Central Location |  |  |
| Troubleshooting Active Directory - Basic and Detailed |  |  |
| Policy Export |  |  |
| Suppression Bypass |  |  |
| Collection Filters |  |  |
| NAD Syslog Correlation in Reports |  |  |
| Time-Range Bound Support Bundles |  |  |
| Guest Activity Monitoring |  |  |
| **Management** |  |  |
| Create a Wildcard Certificate for an ISE deployment |  |  |
| Centralized, Encrypted Backup |  |  |
| Create and run Scheduled or On-Demand Backups |  |  |
| RBAC, with predefined roles, customize, add and remove options, Help desk accounts, super user account. |  |  |
| Centralized Monitoring of All ISE Nodes |  |  |
| Simultaneous Admin Users Logged in & working with ISE |  |  |
| Enable and use External RESTful Services (ERS) APIs |  |  |
| Demonstrate the Upgrading of ISE Nodes with Zero Down Time |  |  |

**Scale & High Availability**

List the scale and HA scenarios you want to test. See [ISE Performance & Scale](http://cs.co/ise-scale) for detailed performance metrics.

|  |  |  |
| --- | --- | --- |
| Scenarios | ✓ Done | Notes |
| **ISE Cube** |  |  |
| Multi-Forest AD Join |  |  |
| Multi-AD within Single Forest Joins |  |  |
| Policy Admin Node (PAN) Down |  |  |
| Policy Service Node (PSN) Down |  |  |
|  |  |  |
| **Survivability & High Availability** |  |  |
| Identity Store (AD) Down/Unavailable |  |  |
| Remote Site WAN Link Down |  |  |
| Reinitialization once WAN is back up |  |  |
| Fail Open |  |  |
| Fail Half-Open (Critical ACL) |  |  |
| Fail Closed |  |  |
|  |  |  |
|  |  |  |

**Policy Details**

List all security policies that are needed to implement the business requirements described above.

Authentication Policy

For each use case (wired, wireless, VPN), describe the authentication policies that will be implemented for all users and endpoints whether managed or unmanaged.

|  |  |  |  |
| --- | --- | --- | --- |
| Rule Name | Condition | Allowed Protocols | ID Store / ID Sequence |
| Device Access | Wired\_MAB | Default Network Access | Internal EndPoints |
| 802.1X Access | Wired\_802.1X | Default Network Access | AD\_then\_Local |
| VPN | NAS-Port-Type = Virtual | Default Network Access | AD |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Default | - | Default Network Access | Internal Users |

Authorization Policy

For each use case (wired, wireless, VPN), describe the authorization policies that will be implemented for all users and endpoints whether managed or unmanaged.

|  |  |  |  |
| --- | --- | --- | --- |
| **Rule Name** | **Identity Groups** | **Other Conditions** | **Permissions** |
| BYOD Unknown | Mobile Devices Logical Group | EAP Tunnel = PEAP  EAP Type = MSCHAPv2 | NSP dACL  NSP Redirect |
| BYOD Registered | Registered | EAP Type = EAP-TLS  SAN = Calling-StationID | Registered dACL |
| IP\_Phones | Cisco-IP-Phones | - | Voice VLAN Authz VVID |
| Printers | Managed-Printers | - | Printer VLAN |
| Cameras | Managed-Cameras | - | Camera VLAN |
| Workstation\_Access | Any | Domain PC | AD Access dACL |
| User\_Role\_1\_Access | Any | Domain Member Role1 | Role1 dACL |
| User\_Role\_2\_Access | Any | Domain Member Role2 | Role2 dACL |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Guest\_Access | Guest | - | Internet Only dACL |
| Default | - | - | Web Auth |

**Resources**

* [ISE Performance & Scale](http://cs.co/ise-scale)
* [ISE Planning & Pre-Deployment Checklists](https://community.cisco.com/t5/security-documents/ise-planning-pre-deployment-checklists/ta-p/3622635)