



Cisco ISE Ports Reference

- [Cisco ISE All Persona Nodes Ports](#), on page 1
- [Cisco ISE Infrastructure](#), on page 1
- [Cisco ISE Administration Node Ports](#), on page 2
- [Cisco ISE Monitoring Node Ports](#), on page 4
- [Cisco ISE Policy Service Node Ports](#), on page 5
- [Cisco ISE pxGrid Service Ports](#), on page 8
- [OCSP and CRL Service Ports](#), on page 9

Cisco ISE All Persona Nodes Ports

Table 1: Ports Used by All Nodes

Cisco ISE Service	Ports on Gigabit Ethernet0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2)
Replication and Synchronization	<ul style="list-style-type: none">• HTTPS (SOAP): TCP/443• Data synchronization/ Replication (JGroups): TCP/12001 (Global)• ISE Messaging Service: SSL: TCP/8671	—

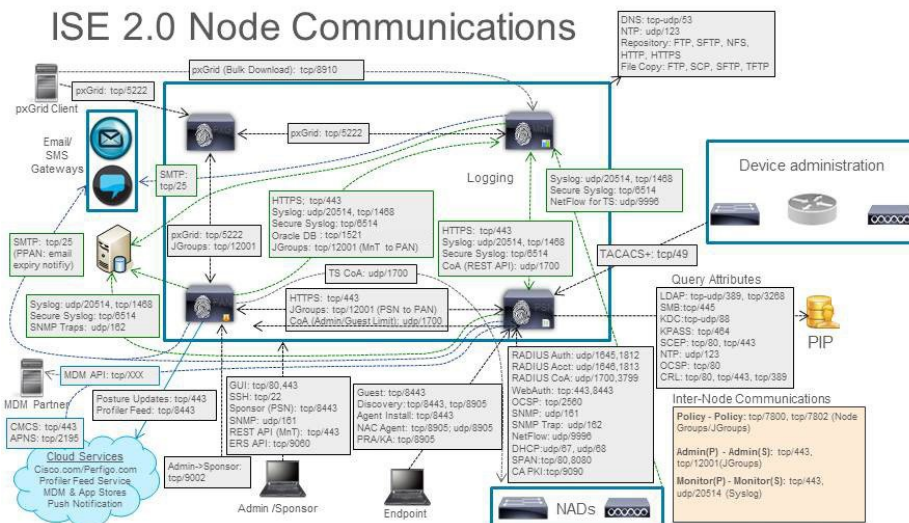
Cisco ISE Infrastructure

This appendix lists the TCP and User Datagram Protocol UDP ports that Cisco ISE uses for intranetwork communications with external applications and devices. The Cisco ISE ports listed in this appendix must be open on the corresponding firewall.

Keep in mind the following information when configuring services on a Cisco ISE network:

- Cisco ISE management is restricted to Gigabit Ethernet 0.

- RADIUS listens on all network interface cards (NICs).
- Cisco ISE server interfaces do not support VLAN tagging. If you are installing on a hardware appliance, ensure that you disable VLAN trunking on switch ports that are used to connect to Cisco ISE nodes and configure them as access layer ports.
- All NICs can be configured with IP addresses.



Cisco ISE Administration Node Ports

The following table lists the ports used by the Administration nodes:

Table 2: Ports Used by the Administration Nodes

Cisco ISE Service	Ports on Gigabit Ethernet0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2)
Administration	<ul style="list-style-type: none"> • HTTP: TCP/80, HTTPS: TCP/443 (TCP/80 redirected to TCP/443; not configurable) • SSH Server: TCP/22 • External RESTful Services (ERS) REST API: TCP/9060 • To manage guest accounts from Admin GUI: TCP/9002 <p>Note Ports 80 and 443 support Admin web applications and are enabled by default.</p> <p>HTTPS and SSH access to Cisco ISE is restricted to Gigabit Ethernet 0.</p>	—
Monitoring	SNMP Query: UDP/161 <p>Note This port is route table dependent.</p>	
Logging (Outbound)	<ul style="list-style-type: none"> • Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 <p>Note Default ports are configurable for external logging.</p> <ul style="list-style-type: none"> • SNMP Traps: UDP/162 	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2)
External Identity Sources and Resources (Outbound)	<ul style="list-style-type: none"> Admin User Interface and Endpoint Authentications: <ul style="list-style-type: none"> LDAP: TCP/389, 3268, UDP/389 SMB: TCP/445 KDC: TCP/88 KPASS: TCP/464 NTP: UDP/123 DNS: UDP/53, TCP/53 <p>Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.</p>	
Email	Guest account and user password expirations email notification: SMTP: TCP/25	

Cisco ISE Monitoring Node Ports

The following table lists the ports used by the Monitoring nodes:

Table 3: Ports Used by the Monitoring Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
Administration	<ul style="list-style-type: none"> HTTP: TCP/80, HTTPS: TCP/443 SSH Server: TCP/22 	—
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 <p>Note This port is route table dependent.</p>	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
Logging	<ul style="list-style-type: none"> • Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 <p>Note Default ports are configurable for external logging.</p> <ul style="list-style-type: none"> • SMTP: TCP/25 for email of alarms • SNMP Traps: UDP/162 	
External Identity Sources and Resources (Outbound)	<ul style="list-style-type: none"> • Admin User Interface and Endpoint Authentications: <ul style="list-style-type: none"> • LDAP: TCP/389, 3268, UDP/389 • SMB: TCP/445 • KDC: TCP/88, UDP/88 • KPASS: TCP/464 • NTP: UDP/123 • DNS: UDP/53, TCP/53 <p>Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.</p>	
Bulk Download for pxGrid	SSL: TCP/8910	

Cisco ISE Policy Service Node Ports

The following table lists the ports used by the Policy Service nodes:

Table 4: Ports Used by the Policy Service Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Administration	<ul style="list-style-type: none"> • HTTP: TCP/80, HTTPS: TCP/443 • SSH Server: TCP/22 • OCSP: TCP/2560 	Cisco ISE management is restricted to Gigabit Ethernet 0.
Clustering (Node Group)	Node Groups/JGroups: TCP/7800	—

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
SCEP	TCP/9090	—
Device Administration	TACACS+: TCP/49	
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 Note This port is route table dependent.	
Logging (Outbound)	<ul style="list-style-type: none"> • Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 Note Default ports are configurable for external logging. <ul style="list-style-type: none"> • SNMP Traps: UDP/162 	
Session	<ul style="list-style-type: none"> • RADIUS Authentication: UDP/1645, 1812 • RADIUS Accounting: UDP/1646, 1813 • RADIUS Change of Authorization (CoA) Send: UDP/1700 • RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799 Note UDP port 3799 is not configurable.	
External Identity Sources and Resources (Outbound)	<ul style="list-style-type: none"> • Admin User Interface and Endpoint Authentications: <ul style="list-style-type: none"> • LDAP: TCP/389, 3268 • SMB: TCP/445 • KDC: TCP/88 • KPASS: TCP/464 • NTP: UDP/123 • DNS: UDP/53, TCP/53 Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
<p>Web Portal Services:</p> <ul style="list-style-type: none"> - Guest/Web Authentication - Guest Sponsor Portal - My Devices Portal - Client Provisioning - Certificate Provisioning - BlackListing Portal 	<p>HTTPS (Interface must be enabled for service in Cisco ISE):</p> <ul style="list-style-type: none"> • Blacklist Portal: TCP/8000-8999 (Default port is TCP/8444.) • Guest Portal and Client Provisioning: TCP/8000-8999 (Default port is TCP/8443.) • Certificate Provisioning Portal: TCP/8000-8999 (Default port is TCP/8443.) • My Devices Portal: TCP/8000-8999 (Default port is TCP/8443.) • Sponsor Portal: TCP/8000-8999 (Default port is TCP/8443.) • SMTP guest notifications from guest and sponsor portals: TCP/25 	
<p>Posture</p> <ul style="list-style-type: none"> - Discovery - Provisioning - Assessment/ Heartbeat 	<ul style="list-style-type: none"> • Discovery (Client side): TCP/80 (HTTP), TCP/8905 (HTTPS) <p>Note By default, TCP/80 is redirected to TCP/8443. See Web Portal Services: Guest Portal and Client Provisioning.</p> <p>Cisco ISE presents the Admin certificate for Posture and Client Provisioning on TCP port 8905.</p> <p>Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use).</p> <ul style="list-style-type: none"> • Discovery (Policy Service Node side): TCP/8443, 8905 (HTTPS) • Provisioning - URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning • Provisioning - Active-X and Java Applet Install including IP refresh, Web Agent Install, and launch NAC Agent Install: See Web Portal Services: Guest Portal and Client Provisioning. • Provisioning - NAC Agent Install: TCP/8443 • Provisioning - NAC Agent Update Notification: UDP/8905 • Provisioning - NAC Agent and Other Package/Module Updates: TCP/8905 (HTTPS) • Assessment - Posture Negotiation and Agent Reports: TCP/8905 (HTTPS) • Assessment - PRA/Keep-alive: UDP/8905 	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Bring Your Own Device (BYOD) / Network Service Protocol (NSP) - Redirection - Provisioning - SCEP	<ul style="list-style-type: none"> • Provisioning - URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning. • Provisioning - Active-X and Java Applet Install (includes the launch of Wizard Install): See Web Portal Services: Guest Portal and Client Provisioning • Provisioning - Wizard Install from Cisco ISE (Windows and Mac OS): TCP/8443 • Provisioning - Wizard Install from Google Play (Android): TCP/443 • Provisioning - Supplicant Provisioning Process: TCP/8905 • SCEP Proxy to CA: TCP/80 or TCP/443 (Based on SCEP RA URL configuration) 	
Mobile Device Management (MDM) API Integration	<ul style="list-style-type: none"> • URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning • API: Vendor specific • Agent Install and Device Registration: Vendor specific 	
Profiling	<ul style="list-style-type: none"> • NetFlow: UDP/9996 Note This port is configurable. • DHCP: UDP/67 Note This port is configurable. • DHCP SPAN Probe: UDP/68 • HTTP: TCP/80, 8080 • DNS: UDP/53 (lookup) Note This port is route table dependent. • SNMP Query: UDP/161 Note This port is route table dependent. • SNMP TRAP: UDP/162 Note This port is configurable. 	

Cisco ISE pxGrid Service Ports

The following table lists the ports used by the pxGrid Service nodes:

Table 5: Ports Used by the pxGrid Service Node

Cisco ISE Service	Ports on Gigabit Ethernet0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
Administration	<ul style="list-style-type: none">• SSL: TCP/5222 (Inter-Node Communication)• SSL: TCP/7400 (Node Group Communication)	—

OCSP and CRL Service Ports

For the Online Certificate Status Protocol services (OCSP) and the Certificate Revocation List (CRL), the ports are dependent on the CA Server or on service hosting OCSP/CRL although references to the Cisco ISE services and ports list basic ports that are used in Cisco ISE Administration Node, Policy Service Node, Monitoring Node separately.

For the OCSP, the default ports that can be used are TCP 80/ TCP 443. Cisco ISE Admin portal expects http-based URL for OCSP services, and so, TCP 80 is the default. You can also use non-default ports.

For the CRL, the default protocols include HTTP, HTTPS, and LDAP and the default ports are 80, 443, and 389 respectively. The actual port is contingent on the CRL server.

