Cisco SNS-3400 Series Appliance Ports Reference

This appendix lists the TCP and User Datagram Protocol UDP ports that Cisco ISE uses for intranetwork communications with external applications and devices.

Table C-1 lists the ports by TCP and UDP port number, identifies the associated feature, service, or protocol, and describes any specific port-related information that applies to the four Gigabit Ethernet ports: GbEth0, GbEth1, GbEth2, and GbEth3. The Cisco ISE ports listed in this table must be open on the corresponding firewall. The ports list provides information that can be useful when configuring a firewall, creating access control lists (ACLs), and configuring services on a Cisco ISE network.

- Cisco ISE management is restricted to Gigabit Ethernet 0.
- RADIUS listens on all network interface cards (NICs).
- All NICs can be configured with IP addresses.

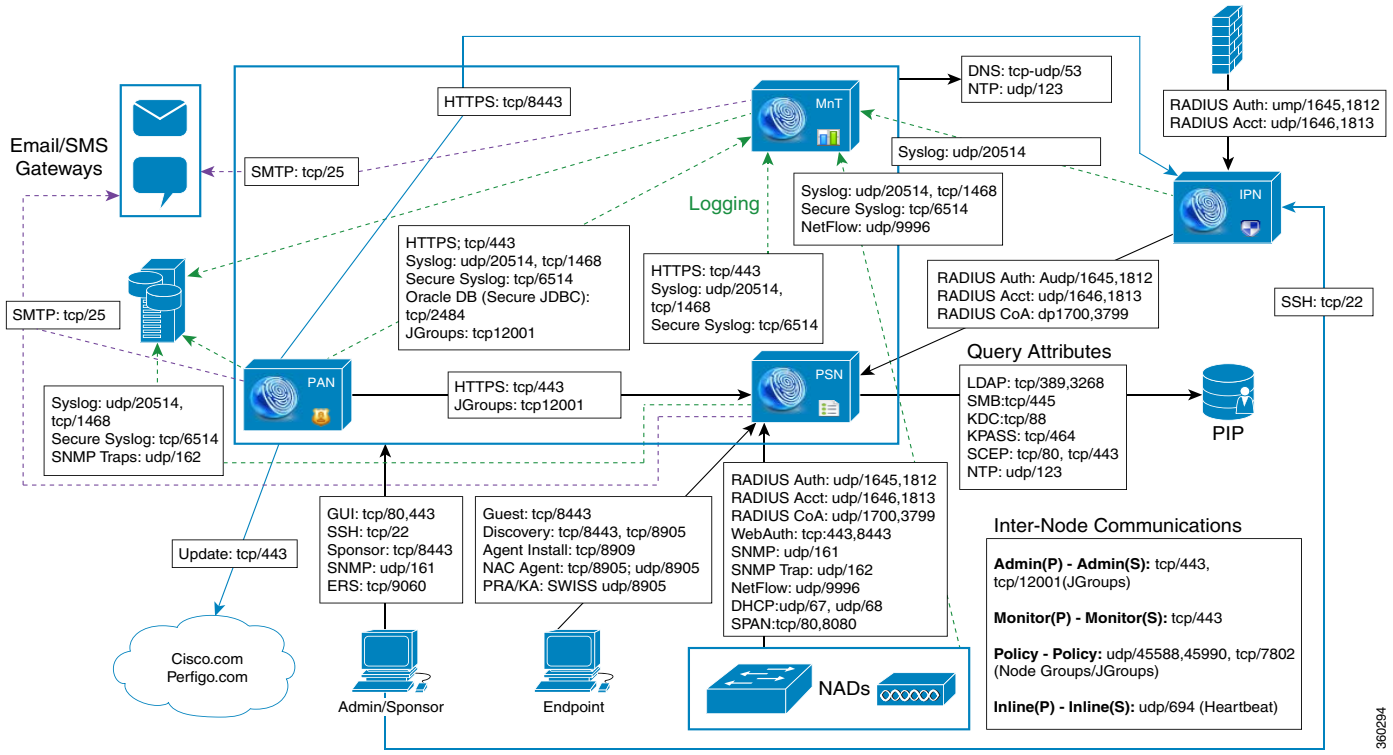

Table C-1 Cisco ISE Services and Ports

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Administration node	Administration	• TCP: 22 (Secure Shell [SSH] server) • TCP: 80[1] (HTTP) • TCP: 443[1] (HTTPS) • TCP: 9060 (External RESTful Services (ERS) REST API) **Note** Port 80 is redirected to port 443 (not configurable). **Note** Ports 80 and 443 support Admin web applications and are enabled by default.	Cisco ISE management is restricted to Gigabit Ethernet 0.	Cisco ISE management is restricted to Gigabit Ethernet 0.	Cisco ISE management is restricted to Gigabit Ethernet 0.
	Replication and Synchronization	• TCP: 443 (HTTPS SOAP) • TCP: 12001 Global (JGroups - Data synchronization / Data replication)	—	—	—
	Monitoring	• UDP: 161 (SNMP Query) **Note** This port is route table dependent.	—	—	—

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
	Logging (Outbound)	• UDP: 20514, TCP: 1468 (Syslog) • TCP: 6514 (Secure Syslog) **Note** Default ports are configurable for external logging. • UDP: 162 (SNMP Traps)—			
	External Identity Stores and Resources	• TCP: 389, 3268, UDP: 389 (LDAP) • TCP: 445 (SMB) • TCP: 88, UDP: 88 (KDC) • TCP: 464 (KPASS) • UDP: 123 (NTP) • TCP: 53, UDP: 53 (DNS) (Admin user interface authentication)	—	—	—
	Guest	Guest account expiry email notification: SMTP: TCP/25			

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Monitoring node	Administration	• TCP: 22 (SSH server) • TCP: 80[1] (HTTP) • TCP: 443[1] (HTTPS)	—	—	—
	Replication and Synchronization	• TCP: 443 (HTTPS SOAP) • TCP: 1521 - Oracle DB Listener • TCP: 12001 Global (JGroups - Data synchronization / Data replication)	• TCP: 1521 - Oracle DB Listener	• TCP: 1521 - Oracle DB Listener	• TCP: 1521 - Oracle DB Listener
	Monitoring	• UDP: 161 (SNMP) **Note** This port is route table dependent.			
	Logging	• UDP: 20514, TCP: 1468 (Syslog) • TCP: 6514 (Secure Syslog) **Note** Default ports are configurable for external logging. • TCP: 25 (SMTP) • UDP: 162 (SNMP Traps)			
	External Resources	• TCP: 389, 3268, UDP: 389 (LDAP) • TCP: 445 (SMB) • TCP: 88, UDP: 88 (KDC) • TCP: 464 (KPASS) • UDP: 123 (NTP) • TCP: 53, UDP: 53 (DNS) (Admin user interface authentication)	—	—	—

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Policy Service node	Administration	• TCP: 22 (SSH server) • TCP: 80[1] (HTTP) • TCP: 443[1] (HTTPS)	—	—	—
	Replication and Synchronization	• TCP: 443 (HTTPS SOAP) • TCP: 12001 Global (JGroups - Data synchronization / Data replication)	—	—	—
	Clustering (Node Group)	• UDP: 45588, 45590 (Local JGroup) • TCP: 7802 (Local JGroup failure detection)	—	—	—
	Monitoring	• UDP: 161 (SNMP) **Note** This port is route table dependent.	—	—	—
	Logging (Outbound)	• UDP: 20514, TCP: 1468 (Syslog) • TCP: 6514 (Secure Syslog) **Note** Default ports are configurable for external logging. • UDP: 162 (SNMP Traps)			
	Session	• UDP:1645, 1812 (RADIUS Authentication) • UDP:1646, 1813 (RADIUS Accounting) • UDP: 1700 (RADIUS change of authorization Send) • UDP: 1700, 3799 (RADIUS change of authorization Listen/Relay) **Note** UDP port 3799 is not configurable.			

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Policy Service node (continued)	External Identity Stores and Resources	• TCP: 389, 3268, (LDAP) • TCP: 445 (SMB) • TCP: 88 (KDC) • TCP: 464 (KPASS) • UDP: 123 (NTP) • UDP: 53 (DNS) (Admin user interface authentication and endpoint authentication)	—	—	—
	Web Portal Services: - Guest/Web Auth - Guest Sponsor portal - My Devices portal - Client Provisioning - BlackListing portal	• HTTPS (Interface must be enabled for service in Cisco ISE.) • TCP: 8000-8999 (Guest Portal and Client Provisioning. Default port is TCP: 8443.) • TCP: 8000-8999 (Sponsor Portal. Default port is TCP: 8443.) • TCP: 8000-8999 (My Devices Portal. Default port is TCP: 8443.) • TCP: 8000-8999 (Blacklist Portal. Default port is TCP: 8444.) • TCP: 25 (SMTP Notification)			

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Policy Service node (continued)	Posture - Discovery - Provisioning - Assessment/ Heartbeat	• TCP: 80 (HTTP) Discovery - Client side • TCP: 8905 (HTTPS) Discovery - Client side **Note** By default, TCP: 80 is redirected to TCP: 8443. See Web Portal Services: Guest Portal and Client Provisioning. • TCP: 8443, 8905 (HTTPS) Discovery - Policy Service node side • URL Redirection—Provisioning. See Web Portal Services: Guest Portal and Client Provisioning. • Active-X and Java Applet Install including IP refresh, Web Agent install, and launch NAC Agent install—Provisioning: See Web Portal Services: Guest Portal and Client Provisioning • TCP: 8443 Provisioning: NAC Agent Install • UDP: 8905 (SWISS) Provisioning: NAC Agent update notification • TCP: 8905 (HTTPS) Provisioning: NAC Agent and other package/module updates • TCP: 8905 (HTTPS) Assessment: Posture Negotiation and Agent Reports • UDP: 8905 (SWISS) Assessment: PRA/Keep-alive			
	Bring Your Own Device (BYOD) / Network Service Protocol - Redirection - Provisioning - SCEP	• URL Redirection—Provisioning. See Web Portal Services: Guest Portal and Client Provisioning • Active-X and Java Applet Install (includes the launch of Wizard Install)—Provisioning. See Web Portal Services: Guest Portal and Client Provisioning • TCP: 8443 Provisioning: Wizard Install from Cisco ISE (Windows and Mac OS) • TCP: 443 Provisioning: Wizard Install from Google Play (Android) • TCP: 8905 Provisioning: Supplicant Provisioning Process • TCP: 80 or TCP: 443 SCEP Proxy to CA (Based on SCEP RA URL config)			
	Mobile Device Management (MDM) API Integration	• URL Redirection—See Web Portal Services: Guest Portal and Client Provisioning • API—Vendor-specific • Agent Install and Device Registration—Vendor-specific			

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Policy Service node (continued)	Profiling	• UDP: 9996 (NetFlow) **Note** This port is configurable. • UDP: 67 (DHCP) **Note** This port is configurable. • UDP: 68 (DHCP SPAN) • TCP: 80, 8080 (HTTP) • NMAP uses ports 0-65535[2] (outbound). • UDP: 53 (DNS lookup) **Note** This port is route table dependent. • UDP: 161 (SNMP Query) **Note** This port is route table dependent. • UDP: 162 (SNMP Trap) **Note** This port is configurable.			
Inline Posture node	Administration	• TCP: 22 (SSH server) • TCP: 8443 (HTTPS) **Note** TCP: 8443 is used by the Administration node.	—	—	—
	Inline Posture	• UDP: 1645, 1812 (RADIUS proxy for authentication) • UDP: 1646, 1813 (RADIUS proxy for accounting) • UDP: 1700, 3799 (RADIUS CoA) **Note** UDP port 3799 is not configurable. • TCP: 9090 (Redirect)	• UDP: 1645, 1812 (RADIUS proxy for authentication) • UDP: 1646, 1813 (RADIUS proxy for accounting) • RADIUS CoA: Not Applicable • TCP: 9090 (Redirect)	—	—
	Logging	• UDP: 20154 (Syslog) **Note** This port is configurable.	• UDP: 20154 (Syslog) **Note** This port is configurable.	—	—

Note Inline Posture node High Availability does not apply to any other Cisco ISE node types.

Table C-1 Cisco ISE Services and Ports (continued)

Cisco ISE Node	Cisco ISE Service	Ports on Gigabit Ethernet 0	Ports on Gigabit Ethernet 1	Ports on Gigabit Ethernet 2	Ports on Gigabit Ethernet 3
Inline Posture node (continued)	High Availability	—	—	UDP: 694 (Heartbeat)	UDP: 694 (Heartbeat)

1. Because Inline Posture nodes do not support the Administration persona, they will not have access to this port.
2. NMAP OS Scan uses ports 0.65535 to detect endpoint operating system

Ports to be Used for OCSP and CRL

For the Online Certificate Status Protocol services (OCSP) and the Certificate Revocation List (CRL), the ports are dependent on the CA Server or service hosting OCSP/CRL although the Cisco ISE Services and ports table above lists basic ports that are used in Cisco ISE.

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 would be the default. You can also use non-default ports.

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

For more information, see *OCSP Services* and *Certificate Store Edit Settings*