Cisco ISE Ports Reference

Cisco ISE All Persona Nodes Ports

Table 1: Ports Used by All Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Replication and Synchronization	• HTTPS (SOAP): TCP/443 • Data Synchronization/ Replication (JGroups): TCP/12001 (Global) • ISE Messaging Service: SSL: TCP/8671 • ISE internal communication: TCP/15672 • Profiler Endpoint Ownership Synchronization/ Replication: TCP/6379	—

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:

- The ports are enabled based on the services that are enabled in your deployment. Apart from the ports that are opened by the services running in ISE, Cisco ISE denies access to all other ports.
- 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.
- The ephemeral port range is from 10000 to 65500. This remains the same for Cisco ISE, Release 2.1 and later.
- VMware on Cloud is supported in Site-to-Site VPN network configuration. Hence, the IP address or port reachability from the network access devices and clients to Cisco ISE must be established without NAT or port filtering.
- All NICs can be configured with IP addresses.
- The policy information point represents the point at which external information is communicated to the Policy Service persona. For example, external information could be a Lightweight Directory Access Protocol (LDAP) attribute.

Related Concepts

Node Types and Personas in Distributed Deployments

Note TCP keep alive time on ISE is 60 minutes. Adjust the TCP timeout values accordingly on the firewall if one exists between ISE nodes.

Operating System Ports

The following table lists the TCP ports that NMAP uses for OS scanning. In addition, NMAP uses ICMP and UDP port 51824.

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99

100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998-2010	2013	2020	2021

2022	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000-4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959
5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689

6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443

44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

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 Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Administration	• HTTPS: TCP/443 • SSH Server: TCP/22 • CoA • External RESTful Services (ERS) REST API: TCP/9060 • • To manage guest accounts from Admin GUI: TCP/9002 • ElasticSearch (Context Visibility; to replicate data from primary to secondary Admin node): TCP/9300 **Note** Port 443 support Admin web applications and are enabled by default. HTTPS and SSH access to Cisco ISE is restricted to Gigabit Ethernet 0. TCP/9300 must be open on both Primary and Secondary Administration Nodes for incoming traffic.	—

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Monitoring	• SNMP Query: UDP/161 **Note** This port is route table dependent. • ICMP	
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SNMP Traps: UDP/162	

External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications:
	  • LDAP: TCP/389, 3268, UDP/389
	  • SMB: TCP/445
	  • KDC: TCP/88
	  • KPASS: TCP/464
	• WMI : TCP/135
	• ODBC:
	Note The ODBC ports are configurable on the third-party database server.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521
	• NTP: UDP/323 (localhost interfaces only)
	• 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 performs an ICMP ping towards DNS while diagnosing the connection against an Active Directory connection.	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Email	Guest account and user password expirations email notification: SMTP: TCP/25	
Smart Licensing	Connection to Cisco cloud over TCP/443 Connection to SSM On-Prem server over TCP/443 and ICMP	

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	• HTTPS: TCP/443 • SSH Server: TCP/22	—
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 **Note** This port is route table dependent. • ICMP	
Logging	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SMTP: TCP/25 for email of alarms • 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 Bond 2)

External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications:
	  • LDAP: TCP/389, 3268, UDP/389
	  • SMB: TCP/445
	  • KDC: TCP/88, UDP/88
	  • KPASS: TCP/464
	• WMI : TCP/135
	• ODBC:
	Note The ODBC ports are configurable on the third-party database server.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521, 15723, 16820
	• NTP: UDP/323 (localhost interfaces only)
	• 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.	

Ports used for inbound communication	• MnT inbound communication from an ISE node with the ISE API Gateway enabled to route the MnT REST APIs: TCP/9443 • TCP/1521: Port 1521 must be enabled for the MnT nodes. Port 1521 is required for inbound communication from PAN. If this port is not enabled for the MnT nodes, MnT node failover might result in loss of logs or reports. **Note** These ports are required in all types of deployments irrespective of being On-Prem or cloud.	
Bulk Download for pxGrid	SSL: TCP/8910	

Cisco ISE Policy Service Node Ports

Cisco ISE supports HTTP Strict Transport Security (HSTS) for increased security. Cisco ISE sends HTTPS responses indicating to browsers that ISE can only be accessed using HTTPS. If users then try to access ISE using HTTP instead of HTTPS, the browser changes the connection to HTTPS before generating any network traffic. This functionality prevents browsers from sending requests to Cisco ISE using unencrypted HTTP before the server can redirect them.

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	• 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	—
SCEP	TCP/9090	—
IPsec/ISAKMP	UDP/500	—
Device Administration	TACACS+: TCP/49 **Note** This port is configurable in Release 2.1 and later releases.	
TrustSec	Use HTTP and Cisco ISE REST API to transfer TrustSec data to network devices over port 9063.	
SXP	• PSN (SXP node) to NADs: TCP/64999 • PSN to SXP (internal communication on the same Cisco ISE): TCP/9644	
TC-NAC	TCP/443	
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 **Note** This port is route table dependent.	
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SNMP Traps: UDP/162	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Session	• RADIUS Authentication: UDP/1645, 1812 • RADIUS Accounting: UDP/1646, 1813 • RADIUS DTLS Authentication/Accounting: UDP/2083. • 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)	• Admin User Interface and Endpoint Authentications:
	  • LDAP: TCP/389, 3268
	  • SMB: TCP/445
	  • KDC: TCP/88
	  • KPASS: TCP/464
	• WMI : TCP/135
	• ODBC:
	Note The ODBC ports are configurable on the third-party database server.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521
	• NTP: UDP/323 (localhost interfaces only)
	• 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.	

Passive ID (Inbound)	• TS Agent: tcp/9094 • AD Agent: tcp/9095 • Syslog: UDP/40514, TCP/11468	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Web Portal Services: - Guest/Web Authentication - Guest Sponsor Portal - My Devices Portal - Client Provisioning - Certificate Provisioning - Blocked List Portal	HTTPS (Interface must be enabled for service in Cisco ISE): • Blocked List 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/8445) • SMTP guest notifications from guest and sponsor portals: TCP/25	
Posture - Discovery - Provisioning - Assessment/ Heartbeat	• Discovery (Client side): TCP/8905 (HTTPS) **Note** Cisco ISE presents the Admin certificate for Posture and Client Provisioning on TCP port 8905. Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use). • Discovery (Policy Service Node side): TCP/8443, 8905 (HTTPS) From Cisco ISE, Release 2.2 or later with AnyConnect, Release 4.4 or later, this port is configurable.	
Bring Your Own Device (BYOD) / Network Service Protocol (NSP) - Redirection - Provisioning - SCEP	• Provisioning - URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning. • For Android devices with EST authentication: TCP/8084. Port 8084 must be added to the Redirect ACL for Android devices. • 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/443 (Based on SCEP RA URL configuration)	
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	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Profiling	• NetFlow: UDP/9996 **Note** This port is configurable. • DHCP: UDP/67 **Note** This port is configurable. • DHCP SPAN Probe: UDP/68 • HTTP: 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 Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
Administration	• SSL: TCP/5222 (Inter-Node Communication) • SSL: TCP/7400 (Node Group Communication)	—
pxGrid Subscribers	TCP/8910	
Inter-node communication	TCP/8910	

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 443. Cisco ISE Admin portal expects http-based URL for OCSP services. You can also use non-default ports.

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

Cisco ISE Processes

The following table lists the Cisco ISE processes and their service impact:

Process Name	Description	Service Impact
Database Listener	Oracle Enterprise Database Listener	Must be in Running state for all services to work properly
Database Server	Oracle Enterprise Database Server. Stores both configuration and operational data.	Must be in Running state for all services to work properly
Application Server	Main Tomcat Server for ISE	Must be in Running state for all services to work properly
Profiler Database	Redis database for ISE Profiling service	Must be in Running state for ISE profiling service to work properly
AD Connector	Active Directory Runtime	Must be in Running state for ISE to perform Active Directory authentications
MnT Session Database	Oracle TimesTen Database for MnT service	Must be in Running state for all services to work properly
MnT Log Collector	Log collector for MnT service	Must be in Running state for MnT Operational Data
MnT Log Processor	Log processor for MnT service	Must be in Running state for MnT Operational Data
Certificate Authority Service	ISE Internal CA service	Must be in Running state if ISE internal CA is enabled

Required Internet URLs

The following table lists the features that use certain URLs. Configure either your network firewall or a proxy server so that IP traffic can travel between Cisco ISE and these resources. If access to any URL listed in the following table cannot be provided, the related feature may be impaired or inoperable.

Table 6: Required URLs Access

Feature	URLs
Posture updates	https://www.cisco.com/ https://iseservice.cisco.com
Profiling Feed Service	https://ise.cisco.com
Smart Licensing	https://tools.cisco.com, in Cisco ISE Release 3.0 Patch 6 and earlier releases https://smartreceiver.cisco.com , in Cisco ISE Release 3.0 Patch 7 and later releases
Telemetry	https://connectdna.cisco.com/
Microsoft Entra ID	login.microsoftonline.com:443 *.login.microsoftonline.com:443 *.login.microsoft.com:443
Social Login for Self-Registered Guests	facebook.co akamaihd.net akamai.co fbcdn.net

The Interactive Help feature needs Cisco ISE to connect to the following URLs using the administration portal browser:

- *.walkme.com
- *.walkmeusercontent.com