



Cisco ISE Network Ports and Protocols Specifications

- [Ports used by all Cisco ISE personas, on page 1](#)
- [Cisco ISE infrastructure requirements, on page 2](#)
- [Operating system ports, on page 3](#)
- [Administration node ports, on page 7](#)
- [Monitoring node ports, on page 10](#)
- [Policy Service node ports, on page 12](#)
- [Cisco pxGrid service ports, on page 15](#)
- [OCSP and CRL service ports, on page 15](#)
- [Cisco ISE processes, on page 16](#)
- [Required internet URLs, on page 17](#)

Ports used by all Cisco ISE personas

Effective communication between Cisco ISE personas, including Policy Administration, Monitoring, and Policy Service nodes, is important to maintaining a resilient and synchronized deployment. To ensure seamless inter-node connectivity and secure data exchange, you must configure the appropriate network ports across your Cisco ISE deployment.

This table lists the essential TCP and UDP ports required for all Cisco ISE personas, for secure communication.

Table 1: Ports used by all Cisco ISE nodes

Cisco ISE service	Ports on Gigabit Ethernet 0 or on Bond 0	Ports on other Ethernet interfaces (Gigabit Ethernet 1–5 or Bond 1 and Bond 2)
Replication and synchronization	<ul style="list-style-type: none"> • HTTPS (SOAP) protocol: TCP port 443 • Data synchronization and replication (JGroups) protocol uses TCP port 12001 (Global) • Cisco ISE messaging service - SSL: TCP port 8671 • Cisco ISE internal communication: TCP port 15672 • Profiler endpoint ownership synchronization and replication: TCP port 6379 	Not applicable

The TCP keepalive interval on Cisco ISE is 60 minutes. If a firewall is deployed between Cisco ISE nodes, configure firewall TCP timeout values accordingly.

Cisco ISE infrastructure requirements

Reliable connectivity between Cisco ISE and your underlying network infrastructure is important for secure operations. These infrastructure ports facilitate essential communication protocols such as RADIUS, TACACS+, and SNMP between Cisco ISE and your network devices.

This section describes the infrastructure requirements and design considerations for deploying Cisco ISE. It outlines management access restrictions, network interface limitations, port and firewall requirements, and supported deployment models to help ensure proper connectivity, policy enforcement, and Cisco ISE operation.

Management interface requirements

Management access to Cisco ISE is restricted to the management interface.

- Management access is allowed only through Gigabit Ethernet 0.
- Administrative access includes the web-based GUI, CLI, and APIs.
- Other network interfaces are not used for management access.

Network interface and VLAN requirements

- Cisco ISE interfaces do not support VLAN tagging.
- Switch ports connected to Cisco ISE nodes must be configured as access ports.
- VLAN trunking must be disabled.

- Each network interface card (NIC) can be assigned a unique IP address.

Ports and firewall requirements

Cisco ISE uses a restricted port model and opens only the ports required by enabled services.

- Ports not explicitly required by active services are denied by default.
- The ephemeral port range used by Cisco ISE is 10000–65500.
- Firewalls must allow required service ports and the ephemeral port range.

RADIUS traffic handling

- RADIUS authentication and accounting traffic is accepted on all available NICs.
- RADIUS traffic is not limited to the management interface.

Cloud and virtual deployment requirements

- VMware on Cloud deployments are supported.
- Connectivity must be provided using a site-to-site VPN.
- Network address translation (NAT) and port filtering are not supported between Cisco ISE nodes and network access devices.

Operating system ports

The NMAP utility is a critical component of Cisco ISE, enabling advanced device profiling and enhanced network visibility. To use this feature effectively, you must ensure that specific TCP ports are open within the network environment. By configuring these ports correctly, Cisco ISE can perform precise operating system identification and comprehensive device classification, which are essential for maintaining a secure and well-managed network infrastructure.

This table lists the TCP ports that NMAP uses for OS scanning. NMAP also uses ICMP and UDP port 51824.

Table 2: Operating system ports

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

Operating system ports

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

Operating system ports

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					

Administration node ports

The Policy Administration node is the primary interface for managing your Cisco ISE deployment. To ensure secure and uninterrupted access to the administrative console and configuration services, specific TCP ports must be configured.

This table lists the ports required for administrative connectivity, helping you maintain secure control over your security policies and system settings.

Table 3: Ports used by the Administration 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 2)
Administration	<ul style="list-style-type: none"> • HTTPS: TCP/443 • SSH Server: TCP/22 • CoA • External RESTful Services (ERS) REST API: , TCP/9060 <p>The ERS and OpenAPI services are HTTPS-only REST APIs and operate over port 443. Currently, ERS APIs also operate over port 9060. This port might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs. The default conn-limit value for port 9060 is 30. If consecutive ERS API calls are returning a HTTP 502 error, we recommend that you increase the conn-limit value of port 9060 to 60 using the command conn-limit cl1 60 port 9060.</p> <ul style="list-style-type: none"> • External RESTful Services (ERS) REST API Certificate-based authentication for DNAC integration mode: TCP/9062 • To manage guest accounts from Admin GUI: TCP/9002 • Port 443 supports Admin web applications and is enabled by default. <p>Access to Cisco ISE via HTTPS and SSH is restricted to Gigabit Ethernet 0.</p> <ul style="list-style-type: none"> • For SAML admin login, Port 8443 of PSN should be reachable from the device where the admin is trying to do the SAML login. 	Not applicable
Monitoring	<ul style="list-style-type: none"> • SNMP Query: UDP/161 <p>This port is route table dependent.</p> <ul style="list-style-type: none"> • ICMP 	

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)
Logging (Outbound)	<ul style="list-style-type: none"> • Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 <p style="margin-left: 20px;">Default ports are configurable for external logging.</p> <ul style="list-style-type: none"> • 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 • KPASS: TCP/464 • WMI : TCP/135 • ODBC: <p style="margin-left: 20px;">The ODBC ports are configurable on the third-party database server.</p> <ul style="list-style-type: none"> • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PostgreSQL: TCP/5432 • Oracle: TCP/1521, TCPS/2484 • NTP: UDP/123 (localhost interfaces only) • DNS: UDP/53, TCP/53 • For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly. • Cisco ISE sends an ICMP ping to the configured DNS server when diagnosing connectivity for an Active Directory connection. 	
Email	Guest account and user password expiration email notification: SMTP: TCP/25	
Smart licensing	<ul style="list-style-type: none"> • Connection to Cisco cloud over TCP/443 • Connection to SSM on-premises server over TCP/443 and ICMP 	

Monitoring node ports

The Monitoring node is important for collecting, storing, and analyzing logs and reports from across your Cisco ISE deployment. To ensure the accurate aggregation of data and the timely generation of system reports, specific ports must be configured to allow communication between the Monitoring Node and other nodes in the cluster.

This table specifies the port requirements essential for maintaining visibility and operational reporting on the Cisco ISE Monitoring node.

Table 4: Ports used by monitoring nodes

Cisco ISE service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on other Ethernet interfaces (Gigabit Ethernet 1 to 5, or Bond 1 and Bond 2)
Administration	<ul style="list-style-type: none"> • HTTPS uses TCP port 443 • SSH Server uses TCP port 22 	Not applicable
Monitoring	<ul style="list-style-type: none"> • Simple Network Management Protocol (SNMP): SNMP uses UDP port 161. This port is route-table-dependent. • ICMP 	
Logging	<ul style="list-style-type: none"> • Syslog uses UDP port 20514 and TCP port 1468 • Secure Syslog uses TCP port 6514 <p>Default ports are configurable for external logging.</p> <ul style="list-style-type: none"> • SMTP uses TCP port 25 for email of alarms • SNMP traps use UDP port 162 	

Cisco ISE service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on other Ethernet interfaces (Gigabit Ethernet 1 to 5, or Bond 1 and Bond 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 uses TCP ports 389 and 3268, and UDP port 389 • SMB uses TCP port 445 • KDC uses TCP port 88 and UDP port 88 • KPASS uses TCP port 464 • WMI uses TCP port 135 • ODBC: <p>The ODBC ports are configurable on the third-party database server.</p> <ul style="list-style-type: none"> • Microsoft SQL uses TCP port 1433 • Sybase uses TCP port 2638 • PostgreSQL uses TCP port 5432 • Oracle uses TCP ports 1521, 15723, and 16820 • NTP uses UDP port 123 (localhost interfaces only) • DNS uses UDP port 53 and TCP port 53 <p>For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.</p>	
Ports used for inbound communication	<p>These ports are required in all types of deployments regardless of being on-premises or in the cloud.</p> <ul style="list-style-type: none"> • MnT node REST APIs: TCP 9443. This allows inbound API requests for monitoring and troubleshooting. • Policy Administration Node (PAN) to MnT: TCP 1521. This enables communication from the PAN to MnT nodes. • OpenAPIs: TCP 443, TCP 9070. These provide access to OpenAPI interfaces for integration. • ERS APIs: TCP 443, TCP 9060. These ports facilitate inbound API requests through ERS interfaces. 	
Bulk download for pxGrid	TCP ports 9993, 2000	

Policy Service node ports

The PSN acts as the primary engine for processing network access requests and enforcing security policies. To ensure consistent authentication, authorization, and accounting services, specific ports must be configured to allow communication with network access devices and endpoints.

Cisco ISE supports HTTP Strict Transport Security (HSTS) to enhance communication security. When enabled, Cisco ISE includes an HSTS header in its HTTPS responses, instructing browsers to interact with the server exclusively over HTTPS. If a user attempts to access Cisco ISE via HTTP, the browser automatically upgrades the connection to HTTPS before transmitting any data. This process prevents unencrypted communication and eliminates the need for server-side redirects.

This table provides a list of ports used by the PSNs.

Table 5: 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"> • HTTPS: TCP port 443 • SSH server: TCP port 22 • OCSP: TCP port 2560 	You can manage the device only through Gigabit Ethernet 0.
Clustering (Node group)	Node groups or JGroups: TCP port 7800	Not applicable
SCEP	TCP port 9090	Not applicable
IPsec or ISAKMP	UDP port 500	Not applicable
Device Administration	TACACS+: TCP port 49	
TrustSec	Use HTTP and Cisco ISE REST API to transfer TrustSec data to network devices over port 9063.	
SXP	<ul style="list-style-type: none"> • PSN (SXP node) to NADs: TCP port 64999 • PSN to SXP (internal communication on the same Cisco ISE): TCP port 9644 	
TC-NAC	TCP port 443	
Monitoring	Simple Network Management Protocol (SNMP): UDP port 161. This port is route table dependent.	
Logging (Outbound)	<ul style="list-style-type: none"> • Syslog: UDP port 20514, TCP port 1468 • Secure Syslog: TCP port 6514 <p>You can configure the default ports for external logging.</p> <ul style="list-style-type: none"> • SNMP traps: UDP port 162 	

Cisco ISE service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on other Ethernet interfaces, or Bond 1, and Bond 2
Session	<ul style="list-style-type: none"> • RADIUS authentication: UDP ports 1645, 1812 • RADIUS accounting: UDP ports 1646, 1813 • RADIUS DTLS authentication and accounting: UDP ports 2083. • RADIUS Change of Authorization (CoA) send: UDP port 1700 • RADIUS Change of Authorization (CoA) listen or relay: UDP ports 1700, 3799 <p>You cannot configure UDP port 3799.</p>	
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 ports 389, 3268 • SMB: TCP port 445 • KDC: TCP port 88 • KPASS: TCP port 464 • WMI : TCP port 135 • ODBC: The ODBC ports are configurable on the third-party database server. <ul style="list-style-type: none"> • Microsoft SQL: TCP port 1433 • Sybase: TCP port 2638 • PostgreSQL: TCP port 5432 • Oracle: TCP port 1521 • NTP: UDP port 123 (localhost interfaces only) • DNS: UDP port 53, TCP port 53 <p>If an external identity source or service is accessible only through an interface other than Gigabit Ethernet 0, configure static routes for that interface.</p>	
Passive ID (Inbound)	<ul style="list-style-type: none"> • TS agent: TCP port 9094 • AD agent: TCP port 9095 • Syslog: UDP port 40514, TCP port 11468 	

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 and web authentication • Guest sponsor portal • My devices portal • Client provisioning • Certificate provisioning • Blocked list portal 	<p>HTTPS (Interface must be enabled for service in Cisco ISE):</p> <ul style="list-style-type: none"> • Blocked list portal: TCP port 8000-8999 (default port is TCP port 8444) • Guest portal and client provisioning: TCP port 8000-8999 (default port is TCP port 8443) • Certificate provisioning portal: TCP port 8000-8999 (default port is TCP port 8443) • My devices portal: TCP port 8000-8999 (default port is TCP port 8443) • Sponsor portal: TCP portal 8000-8999 (default port is TCP portal 8445) • SMTP guest notifications from guest and sponsor portals: TCP portal 25 	
<p>Posture</p> <ul style="list-style-type: none"> • Discovery • Provisioning • Assessment or heartbeat 	<ul style="list-style-type: none"> • Discovery (Client side): TCP port 8905 (HTTPS) <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> <p>From Cisco ISE release 3.1, port 8905 is disabled by default on non-PSNs. To enable this port, check the Enable Port 8905 on non-Policy Service Nodes for Posture Services check box in the General Settings window (Administration > System > Settings > Posture > General Settings).</p> <ul style="list-style-type: none"> • Discovery (Policy Service Node side): TCP port 8443, 8905 (HTTPS) . This is configurable in the latest Cisco ISE release with Cisco Secure Client release 4.4 and later. • Assessment - Posture negotiation and agent reports: TCP port 8905 (HTTPS) • Bidirectional posture flow - TCP port 8000-8999 (default port is TCP port 8449) 	
<p>Bring Your Own Device (BYOD) or Network Service Protocol (NSP)</p> <ul style="list-style-type: none"> • Redirection • Provisioning • SCEP 	<ul style="list-style-type: none"> • Provisioning - URL redirection: See web portal services: Guest portal and client provisioning • For android devices with EST authentication: TCP port 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 port 8443 • Provisioning - Wizard install from Google Play (Android): TCP port 443 • Provisioning - Supplicant provisioning process: TCP port 8905 • SCEP proxy to CA: TCP port 443 (Based on SCEP RA URL configuration) 	

Cisco ISE service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on other Ethernet interfaces, or Bond 1, and Bond 2
Mobile Device Management (MDM) API integration	<ul style="list-style-type: none"> Provisioning - 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 port 9996 can be configured DHCP: UDP port 67 can be configured DHCP SPAN Probe: UDP/68 HTTP: 8080 DNS: UDP port 53 (lookup). This port is route table dependent. SNMP query: UDP port 161. This port is route table dependent. SNMP trap: UDP port 162 can be configured. 	

Cisco pxGrid service ports

Cisco pxGrid enables the secure exchange of contextual information between Cisco ISE and integrated third-party security platforms. You must enable specific ports to allow these integrations and ensure seamless data sharing.

From Cisco ISE release 3.1, all pxGrid connections must use version 2.0. Integrations that rely on pxGrid version 1.0 (XMPP-based) are no longer operational. We recommend upgrading your other systems to Cisco pxGrid 2.0-compliant versions to avoid potential disruptions to integrations.

This table lists the ports used by Cisco pxGrid service nodes.

Table 6: Ports used by Cisco pxGrid service 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)
pxGrid subscribers	TCP port 8910	
Inter-node communication	TCP port 8910	

OCSP and CRL service ports

Cisco ISE uses OCSP and CRL services to check the revocation status of client and server certificates against trusted Certificate Authorities (CA).

The ports required for Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) services depend on the CA server or the service hosting OCSP or CRL. Cisco ISE services and ports documentation lists the basic ports used by the Cisco ISE administration node, monitoring node, and policy service node separately.

For OCSP, the default port is TCP 443. The Cisco ISE Admin portal accepts HTTP-based URLs for OCSP services. Non-default ports can also be used.

For CRL, the default protocols are HTTP, HTTPS, and LDAP. The default ports are 443 (HTTPS) and 389 (LDAP), respectively. The actual port depends on the CRL server.

Cisco ISE processes

Cisco ISE uses specialized background processes to manage authentication, policy enforcement, system monitoring, and database synchronization. By understanding these services, you can troubleshoot issues, tune performance, and maintain the stability of your deployment.

This table lists the Cisco ISE processes and their service impact.

Process name	Description	Service impact
Database listener	Oracle Enterprise Database listener	You must ensure that this process is running for all services to work properly.
Database server	Oracle Enterprise Database server, which stores both configuration and operational data	You must ensure that this process is running for all services to work properly.
Application server	Main Tomcat server for Cisco ISE	You must ensure that this process is running for all services to work properly.
Profiler database	Redis database for Cisco ISE profiling service	You must ensure that this process is running for all services to work properly.
AD connector	Active Directory runtime	You must ensure that this process is running for all services to work properly.
MnT session database	Oracle TimesTen Database for monitoring and troubleshooting (MnT) service	You must ensure that this process is running for all services to work properly.
MnT log collector	Log collector for MnT service	You must ensure that this process is running to support MnT operational data.
MnT log processor	Log processor for MnT service	You must ensure that this process is running to support MnT operational data.
Certificate Authority service	Cisco ISE Internal Certificate Authority (CA) service	You must ensure that this process is running if Cisco ISE internal Certificate Authority (CA) is enabled.

Required internet URLs

Cisco ISE requires connectivity to specific external internet services to maintain up-to-date threat intelligence, license compliance, and cloud-integrated functionality. To ensure these services operate correctly, you must allow access to these URLs through their network firewalls.

This table lists the features that use certain URLs. You must configure either your network firewall or a proxy server so that IP traffic can travel between Cisco ISE and these resources. If you cannot provide access to a required URL, the related feature may not work as intended.

Configure your network firewall or proxy server to allow IP traffic between Cisco ISE and these resources. If access to any required URL is not possible, the feature may not function as intended.

Table 7: Required internet URLs

Feature	URLs
Posture updates	https://www.cisco.com/ https://iseservice.cisco.com
Profiling feed service	https://ise.cisco.com
Smart licensing	https://smartreceiver.cisco.com
Telemetry	https://connectdna.cisco.com/
Connection from Cisco ISE to Cisco pxGrid Cloud Portal	https://dna.cisco.com https://dnaservices.cisco.com https://ciscodnacloud.com
Cisco AI analytics	http://api.use1.prd.kairos.ciscolabs.com for the US East region http://api.euc1.prd.kairos.ciscolabs.com for EU central region Network connectivity to these required URLs is through HTTPS, TCP port 443.
Microsoft Entra ID	graph.microsoft.com login.microsoftonline.com:443 *.login.microsoftonline.com:443 *.login.microsoft.com:443
Workload connector	public.ecr.aws
Social login for self-registered guests	facebook.co akamaihd.net akamai.co fbcdn.net

Required internet URLs

Feature	URLs
Cisco DUO integration for multifactor authentication	*.duosecurity.com:443

The **Interactive Help** feature requires Cisco ISE to connect to these URLs through the administration portal browser:

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