Cisco ISE Ports Reference

- Cisco ISE All Persona Nodes Ports, on page 1
- Cisco ISE Infrastructure, on page 2
- Operating System Ports, on page 2
- Cisco ISE Administration Node Ports, on page 6
- Cisco ISE Monitoring Node Ports, on page 10
- Cisco ISE Policy Service Node Ports, on page 13
- Cisco ISE pxGrid Service Ports, on page 17
- OCSP and CRL Service Ports, on page 18
- Cisco ISE Processes, on page 18
- Required Internet URLs, on page 19

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 (Gigabit Ethernet 1 through 5, or Bond 1 and 2)
Replication and Synchronization	• HTTPS (SOAP): TCP/443 • Data Synchronization and 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 section lists the TCP and UDP ports that Cisco ISE uses for communication with external applications and devices. Ensure that the firewall allows these Cisco ISE ports.

Consider these points when configuring services on a Cisco ISE network:

- Cisco ISE enables ports according to the services active in your deployment. Cisco ISE denies access to all other ports
- Management access to Cisco ISE is allowed only through Gigabit Ethernet 0 (zero).
- RADIUS accepts connections on all network interface cards (NICs).
- Cisco ISE server interfaces do not support VLAN tagging. If you install Cisco ISE on a hardware appliance, disable VLAN trunking on switch ports for Cisco ISE node connections. Configure these ports as access ports.
- The ephemeral port range is from 10000 to 65500.
- VMware on Cloud is supported in Site-to-Site VPN network configuration. Ensure that network access devices and clients can reach Cisco ISE IP addresses or ports directly, without NAT or port filtering.
- You can configure an IP address on each NIC.
- 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

This table lists the TCP ports that NMAP uses for OS scanning. NMAP also 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

This 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 (Gigabit Ethernet 1 through 5, or Bond 1 and 2)
Administration		—

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)
	• HTTPS: TCP/443 • SSH Server: TCP/22 • CoA • External RESTful Services (ERS) REST API: TCP/9060 **Note** The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. Currently, ERS APIs also operate over port 9060. However, port 9060 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**. • External RESTful Services (ERS) REST API Certificate-based authentication for DNAC integration mode: TCP/9062 • 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 supports Admin web applications and is enabled by default. Access to Cisco ISE via HTTPS and SSH is restricted to Gigabit Ethernet 0. TCP/9300 must be open on both Primary and Secondary Administration Nodes for incoming traffic. **Note** For SAML admin login, Port 8443 of PSN	

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)
	should be reachable from the device where the admin is trying to do the SAML login.	
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	

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)	• 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
	  • PostgreSQL: TCP/5432
	  • Oracle: TCP/1521, TCPS/2484
	• NTP: UDP/123 (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.	

Email	Guest account and user password expiration 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

Use this table to find the ports required for 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 to 5, or Bond 1 and Bond 2)
Administration	• HTTPS uses TCP port 443. • SSH Server uses TCP port 22.	—
Monitoring	Simple Network Management Protocol [SNMP]: SNMP uses UDP port 161. **Note** This port is route-table-dependent. • ICMP	
Logging	• Syslog uses UDP port 20514 and TCP port 1468. • Secure Syslog uses TCP port 6514. **Note** Default ports are configurable for external logging. • 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)	• Admin User Interface and Endpoint Authentications:
	  • 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:
	Note
	The ODBC ports are configurable on the third-party database server.
	  • 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.
	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 a Cisco ISE node with the ISE API Gateway enabled to route the MnT REST APIs uses TCP port 9443. • Enable TCP port 1521 on the MnT nodes. This port is required for inbound communication from the Policy Administration Node (PAN). • Enable TCP port 443 globally and TCP port 9070 between nodes in the deployment for Open APIs. • Enable TCP ports 443 and 9060 for ERS APIs. **Note** These ports are required in all types of deployments regardless of being on-premises or in the cloud.	

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)
Bulk Download for pxGrid	TCP/9993, 2000	
LogAnalytics(Kibana)	Open port 5,701 on MnT nodes for communication with PAN nodes.	

Cisco ISE Policy Service Node Ports

Cisco ISE supports HTTP Strict Transport Security (HSTS) for increased security. The system sends HTTPS responses, instructing browsers to access ISE only with HTTPS. If a user attempts to access ISE with HTTP, the browser switches the connection to HTTPS before any network traffic is generated. This functionality stops browsers from sending requests over unencrypted HTTP. As a result, the server does not need to perform a redirect.

The 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.	You can manage the device only through Gigabit Ethernet 0.
Clustering (Node Group)	Node Groups/JGroups: TCP/7800	—
SCEP	TCP/9090	—
IPsec/ISAKMP	UDP/500	—
Device Administration	TACACS+: TCP/49	
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.	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SNMP Traps: UDP/162	
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.	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2

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
	  • PostgreSQL: TCP/5432
	  • Oracle: TCP/1521
	• NTP: UDP/123 (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	
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	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
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). From Cisco ISE 3.1 onwards, port 8905 is disabled by default on non-Policy Service nodes. 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**). • 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. • Assessment - Posture Negotiation and Agent Reports: TCP/8905 (HTTPS) • Bidirectional Posture Flow - TCP/8000-8999 (default port is TCP/8449)	
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

Note From Cisco Identity Services Engine (ISE) Release 3.1, all pxGrid connections must use Version 2.0. Integrations that rely on pxGrid Version 1.0 (XMPP-based) will no longer function after Cisco Identity Services Engine Release 3.1.

We recommend upgrading your other systems to pxGrid 2.0-compliant versions to avoid potential disruptions to integrations.

This table lists the ports used by 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)
pxGrid Subscribers	TCP port 8910	

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)
Inter-node communication	TCP port 8910	

OCSP and CRL Service Ports

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. The ISE services and ports documentation lists the basic ports used by the ISE Administration Node, Monitoring Node, and Inline Posture Node separately.

For the OCSP, the default port is TCP 443. The 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

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

Process Name	Description	Service Impact
Database Listener	Oracle Enterprise Database Listener.	The process must be in the running state for all services to work properly.
Database Server	Oracle Enterprise Database Server, which stores both configuration and operational data.	The process must be in the running state for all services to work properly.
Application Server	Main Tomcat Server for Identity Services Engine (ISE)	Must be in running state for all services to work properly
Profiler Database	Redis database for Identity Services Engine (ISE) Profiling service.	The process must be in the running state for the Identity Services Engine (ISE) profiling service to work properly.
AD Connector	Active Directory Runtime.	The process must be in the running state for Identity Services Engine (ISE) to perform Active Directory authentications.
MnT Session Database	Oracle TimesTen Database for Monitoring and Troubleshooting (MnT) service.	Must be in Running state for all services to work properly.
MnT Log Collector	Log collector for Monitoring and Troubleshooting (MnT) service.	The process must be in the running state to support MnT operational data.
MnT Log Processor	Log processor for MnT service.	Must be in Running state for Monitoring and Troubleshooting (MnT) Operational Data.

Certificate Authority Service	Identity Services Engine (ISE) Internal Certificate Authority (CA) service.	The process must be in the running state if the Identity Services Engine (ISE) internal Certificate Authority (CA) is enabled.

Required Internet URLs

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 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://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 the 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
Social Login for Self-Registered guests	facebook.co akamaihd.net akamai.co fbcdn.net

Feature	URLs
Customer Experience Surveys in Cisco ISE	From Cisco ISE Release 3.2 Patch 4, browser access to *.qualtrics.com is required.

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

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