Security, Internet Access, and Communication Ports

The following topics provide information on system security, internet access, and communication ports:

Security and Hardening

To safeguard the management center, you should install it on a protected internal network. Although the management center is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it (or any managed devices) from outside the firewall.

If the management center and its managed devices reside on the same network, you can connect the management interfaces on the devices to the same protected internal network as the management center. This allows you to securely control the devices from the management center. You can also configure multiple management interfaces to allow the management center to manage and isolate traffic from devices on other networks.

Regardless of how you deploy your appliances, inter-appliance communication is encrypted. However, you must still take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or man-in-the-middle attack.

Communication Ports

For deployments behind a network barrier—like an edge firewall—make sure you allow traffic on the required ports. Note that ports not required for essential or default operations remain closed until needed by a configuration or feature.

Ports for Management Center

The management center uses these ports to communicate.

Table 1: Inbound Ports for Management Center

Inbound Port	Protocol/Feature	Details
22/tcp	SSH	Secure remote connections to the appliance.
161/udp	SNMP	Allow access to MIBs via SNMP polling.
443/tcp	HTTPS	**Required.** Access the management center web interface.
443/tcp	HTTPS	Onboard an on-prem management center to CDO with Secure Device Connector (on-prem).
443/tcp	HTTPS	Communicate with integrated and third-party products using the REST API.
443/tcp	HTTPS	Integrate with Secure Endpoint.
623/udp	SOL/LOM	Lights-Out Management (LOM) using a Serial Over LAN (SOL) connection.
1500/tcp 2000/tcp	Database access	Allow read-only access to the event database by a third-party client.
8302/tcp	eStreamer	Communicate with an eStreamer client.
8305/tcp	Appliance communications	**Required.** Securely communicate with managed devices. Also initiates connections on this port. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8307/tcp	Host input client	Communicate with a host input client.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics. Also initiates connections on this port.

Table 2: Outbound Ports for Management Center

Outbound Port	Protocol/Feature	Details
7/udp 514/udp 6514/tcp	Syslog (audit logging)	Verify connectivity with the syslog server when configuring audit logging (7/udp). Send audit logs to a remote syslog server, when TLS is not configured (514/udp). Send audit logs to a remote syslog server, when TLS is configured (6514/tcp).
25/tcp	SMTP	Send email notices and alerts.
53/tcp 53/udp	DNS	**Required.** DNS

Outbound Port	Protocol/Feature	Details
67/udp 68/udp	DHCP	DHCP
80/tcp	HTTP	Send and receive data from the internet. See Internet Resources Accessed, on page 5.
80/tcp	HTTP	Download custom Security Intelligence feeds over HTTP.
80/tcp	HTTP	Download or query URL category and reputation data. This feature also uses 443/tcp.
80/tcp	HTTP	Display RSS feeds in the dashboard.
123/udp	NTP	Synchronize time.
162/udp	SNMP	Send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	Communicate with an LDAP server for external authentication. Obtain metadata for detected LDAP users. Configurable.
443/tcp	HTTPS	Send and receive data from the internet. See Internet Resources Accessed, on page 5.
443/tcp	HTTPS	Communicate with the Secure Malware Analytics Cloud (public or private).
443/tcp	HTTPS	Integrate with Secure Endpoint. Also accepts connections on this port.
443/tcp	HTTPS	Onboard an on-prem management center to CDO with Cisco Security Cloud or Secure Device Connector (cloud).
1812/udp 1813/udp	RADIUS	Communicate with a RADIUS server for external authentication and accounting. Configurable.
5222/tcp	ISE	Communicate with an ISE identity source.
8305/tcp	Appliance communications	**Required.** Securely communicate with managed devices. Also accepts connections on this port. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics. Also accepts connections on this port.
8989/tcp	Cisco Success Network	Transmit usage information and statistics.

Ports for Managed Devices

Managed devices use these ports to communicate.

Table 3: Inbound Ports for Managed Devices

Inbound Port	Protocol/Feature	Details
22/tcp	SSH	Secure remote connections to the appliance.
161/udp	SNMP	Allow access to MIBs via SNMP polling.
443/tcp	HTTPS	Communicate with integrated and third-party products using the REST API.
443/tcp	Remote access VPN (SSL/IPSec)	Allow secure VPN connections to your network from remote users.
500/udp 4500/udp	Remote access VPN (IKEv2)	Allow secure VPN connections to your network from remote users.
885/tcp	Captive portal	Communicate with a captive portal identity source.
8305/tcp	Appliance communications	**Required.** Securely communicate with the management center. Also initiates connections on this port. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests. Also initiates connections on this port.

Table 4: Outbound Ports for Managed Devices

Outbound Port	Protocol/Feature	Details
53/tcp 53/udp	DNS	DNS
67/udp 68/udp	DHCP	DHCP
123/udp	NTP	Synchronize time.
162/udp	SNMP	Send SNMP alerts to a remote trap server.
1812/udp 1813/udp	RADIUS	Communicate with a RADIUS server for external authentication and accounting. Configurable.
389/tcp 636/tcp	LDAP	Communicate with an LDAP server for external authentication. Configurable.

Outbound Port	Protocol/Feature	Details
443/tcp	HTTPS	Send and receive data from the internet; see Internet Resources Accessed, on page 5.
514/udp	Syslog (audit logging)	Send audit logs to a remote syslog server, when TLS is not configured.
8305/tcp	Appliance communications	**Required.** Securely communicate with the management center. Also accepts connections on this port. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8514/udp	Secure Network Analytics Manager	Send syslog messages to Secure Network Analytics using Security Analytics and Logging (On Premises).
8989/tcp	Cisco Support Diagnostics	Transmits usage information and statistics. Also accepts connections on this port.

Internet Resources Accessed

In addition to the system accessing the internet, your browser may contact Google (google.com) or Amplitude (amplitude.com) web analytics servers to provide non-personally-identifiable usage data to Cisco.

Internet Resources Accessed by Management Center

The management center connects to the internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP). You can configure a proxy server, except for NTP and whois. For some features, your location determines which resources you access. Some features also require device access; see the next table.

Table 5: Internet Resources Accessed by Management Center

Feature	Reason	High Availability	Resource
CA certificate bundles	Queries for new CA certificates at a daily system-defined time. The local CA bundle contains certificates to access several Cisco services. Requires Version 7.2.4.	Each peer downloads its own certificates.	cisco.com/security/pki

Feature	Reason	High Availability	Resource
Malware defense	Secure Malware Analytics Cloud lookups.	Both peers perform lookups.	Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations
	Download signature updates for file preclassification and local malware analysis.	Active peer downloads, syncs to standby.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Query for dynamic analysis results.	Both peers query for dynamic analysis reports.	fmc.api.threatgrid.com fmc.api.threatgrid.eu
Security intelligence	Download security intelligence feeds.	Active peer downloads, syncs to standby.	intelligence.sourcefire.com
URL filtering	Download URL category and reputation data. Manually query (look up) URL category and reputation data. Query for uncategorized URLs.	Active peer downloads, syncs to standby.	URLs: • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com IPv4 blocks: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 blocks: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Secure Endpoint	Receive malware events detected by Secure Endpoint from the cloud. Display malware events detected by the system in Secure Endpoint. Use centralized file Block and Allow lists created in Secure Endpoint to override dispositions from the cloud.	Both peers receive events. You must also configure the cloud connection on both peers (configuration is not synced).	Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations

Feature	Reason	High Availability	Resource
Cisco Smart Software Manager	Communicate with the Smart Software Manager.	Active peer communicates.	www.cisco.com 7.2.0–7.2.9: tools.cisco.com:443 7.2.10–7.2.x: smartreceiver.cisco.com
Cisco Success Network	Transmit usage information and statistics.	Active peer communicates.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics.	Active peer communicates.	api-sse.cisco.com:8989
Cisco XDR integration	Configure devices to send events to the Cisco Security Cloud.	Active peer communicates.	Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide
Time synchronization	Synchronize time in your deployment. Not supported with a proxy server.	Both peers communicate with the NTP server.	User configured
RSS feeds	Display the Cisco Threat Research Blog on the dashboard.	Both peers communicate.	blog.talosintelligence.com blogs.cisco.com feeds.feedburner.com
Upgrades	Download product (management center and device) upgrades.	Upgrade packages do not sync.	7.2.0–7.2.5: support.sourcefire.com 7.2.6–7.2.x: cdo-ftd-images3-us-west-2.amazonaws.com
Intrusion rules	Download intrusion rules (SRU/LSP).	Active peer downloads, syncs to standby.	talosintelligence.com
Vulnerability database	Download VDB updates.	Active peer downloads, syncs to standby.	support.sourcefire.com
Geolocation database	Download GeoDB updates.	Active peer downloads, syncs to standby.	support.sourcefire.com

Feature	Reason	High Availability	Resource
Whois	Request whois information for an external host. Not supported with a proxy server.	Any appliance requesting whois information must have internet access.	The whois client tries to guess the right server to query. If it cannot guess, it uses: • NIC handles: whois.networksolutions.com • IPv4 addresses and network names: whois.arin.net

Internet Resources Accessed by Managed Devices

Managed devices connect to the internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP). You can configure a proxy server, except for NTP. For some features, your location determines which resources you access.

Table 6: Internet Resources Accessed by Managed Devices

Feature	Reason	High Availability/Clustering	Resource
CA certificate bundles	Queries for new CA certificates at a daily system-defined time. The local CA bundle contains certificates to access several Cisco services. Requires Version 7.2.4.	Each unit downloads its own certificates.	cisco.com/security/pki
Malware defense	Submit files for dynamic analysis.	All units submit files.	fmc.api.threatgrid.com fmc.api.threatgrid.eu
Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics.	All units communicate.	api-sse.cisco.com:8989
Time synchronization	Synchronize time in your deployment. Not supported with a proxy server.	All units communicate with the NTP server.	User configured.
Cisco XDR integration	Send events to the Cisco Security Cloud.	All units send events.	Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide