

Communication Ports and Internet Access

- Communication ports for managed devices, on page 1
- Internet access requirements for managed devices, on page 2
- Internet resources accessed by your browser, on page 4

Communication ports for managed devices

Managed devices use these ports to communicate. 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.

Inbound ports for managed devices

Managed devices accept inbound traffic on these ports.

Table 1: Inbound ports for managed devices

Inbound port	Protocol/Feature	Details
Required for specific configurations or features		
22/tcp	SSH	Secure remote connections to the appliance.
161/udp	SNMP	Allow access to MIBs via SNMP polling.
443/tcp	Remote access VPN (SSL)	Allow secure VPN connections to your network from remote users.
443/udp	Remote access VPN (DTLS)	Allow secure VPN connections to your network from remote users.
500/udp 4500/udp	Remote access VPN (IKEv2) and site-to-site VPN	Allow secure VPN connections to your network from remote users and remote VPN peers.
885/tcp	Captive portal	Communicate with a captive portal identity source.

Outbound ports for managed devices

Managed devices initiate outbound traffic on these ports. Managed devices also use ephemeral source ports for TCP and UDP traffic that they initiate. Make sure intervening network barriers allow response traffic for these connections.

Table 2: Outbound ports for managed devices

Outbound port	Protocol/Feature	Details
Required for initial setup		
53/tcp 53/udp	DNS	DNS
123/udp	NTP	Synchronize time.
443/tcp	HTTPS	Send and receive data from the internet; see Internet access requirements for managed devices, on page 2 for a list of resources that the device needs to access. Also accepts connections on this port.
8305/tcp	Appliance communications	Securely communicate with the Cloud-Delivered Firewall Management Center.
Required for specific configurations or features		
67/udp 68/udp	DHCP	DHCP
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.
514/udp	Syslog (audit logging)	Send audit logs to a remote syslog server, when TLS is not configured.
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	Port 8989/tcp is used only for local/on-box communication between Cisco Support Diagnostics and SSEConnector. Cisco Support Diagnostics cloud/CDX communication is proxied through SSEConnector and uses HTTPS/WSS on 443/tcp externally.

Internet access requirements for managed devices

Internet access to the listed resources supports essential operations and configured features in your deployment.

For deployments behind a network barrier—like an edge firewall—make sure you allow traffic on the required ports to the listed resources.

Internet resources accessed by managed devices

This table identifies the internet resources that managed devices access.

Table 3: Internet resources for managed devices

Feature	Reason	HA/Clustering	Port	Resource
Required for initial setup				
DNS	DNS	All units communicate with the DNS server.	53/tcp 53/udp	Default OpenDNS servers: 208.67.222.222 and 208.67.220.220 2620:119:35::35
NTP	Synchronize time. Not supported with a proxy server.	All units communicate with the NTP server.	123/udp	Default NTP servers: 0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
Required for general operations				
CA certificate bundles	Managed devices query for new CA certificates daily at a system-defined time. The local CA bundle contains certificates for accessing several Cisco services.	Each unit downloads its own certificates.	443/tcp	cisco.com/security/pki
Cisco Support Diagnostics	Cisco Support Diagnostics receives authorized CSD/CDX troubleshooting requests and uploads generated troubleshooting files through SSEConnector. External Cisco cloud connectivity utilizes HTTPS/WSS on 443/tcp.	All units communicate.	443/tcp	api-sse.cisco.com
Required for specific configurations or features				
Malware Defense	Submit files for dynamic analysis.	All units submit files.	443/tcp	fmc.api.threatgrid.com fmc.api.threatgrid.eu

Feature	Reason	HA/Clustering	Port	Resource
Upgrades	Download upgrades directly to managed devices. Tests the connection once a week.	Upgrade packages do not sync. Each unit must get its own.	443/tcp	cdo-fdi-images3-us-west-2.amazonaws.com
Umbrella DNS	Direct DNS queries to Cisco Umbrella for validation and policy enforcement.	All units communicate.	443/tcp	api.opendns.com

Security Cloud Control regional IP addresses

To onboard and manage devices using zero-touch provisioning, allow inbound access on port 443 (or whichever port you configured for device management) from the Security Cloud Control IP addresses in your region.

Table 4: Security Cloud Control IP addresses by region

Security Cloud Control region	IP addresses
Asia-Pacific-Japan (APJ)	54.199.195.111 52.199.243.0
Australia (AUS)	13.55.73.159 13.238.226.118
Europe, the Middle East, or Africa (EMEA)	35.157.12.126 35.157.12.15
India (IN)	35.154.115.175 13.201.213.99
United States (US)	52.34.234.2 52.36.70.147

Internet resources accessed by your browser

When you use the Cloud-Delivered Firewall Management Center, your browser may contact Google (google.com) or Amplitude (amplitude.com) web analytics servers to send non-personally-identifiable usage data to Cisco. For browser compatibility information, refer to the *Cisco Secure Firewall Management Center Compatibility Guide*.