Security, Internet Access, and Communication Ports

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

Communication Ports for Managed Devices

Managed devices use the following 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.

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.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests. Also initiates connections on this port.

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 Resources Accessed by 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 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	Transmits usage information and statistics. Also accepts connections on this port.

Internet Resources Accessed by Managed Devices

Managed devices access the following outside resources. For deployments behind a network barrier—like an edge firewall—make sure you allow traffic on the required ports to the listed resources. In addition to managed devices accessing the internet, your browser may contact Amplitude (amplitude.com) web analytics servers to provide non-personally-identifiable usage data to Cisco.

Table 3: Internet Resources Accessed by 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	The following are the 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	The following are the 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	The local CA bundle contains certificates to access several Cisco services. Queries for new CA certificates at a daily system-defined time.	Each unit downloads its own certificates.	443/tcp	cisco.com/security/pki
Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics.	All units communicate.	443/tcp	api-sse.cisco.com:8989
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
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-ftd-images.s3-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

To onboard and manage devices using zero-touch provisioning, ensure that you allow inbound access on port 443 (or whichever port you have configured for your device management) to the following IP addresses that are associated to Security Cloud Control:

Security Cloud Control Region	IP
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