Users should complete the tasks listed in the chapter *Get Started with Prime Infrastructure chapter* in the latest Cisco Prime Infrastructure User Guide . After you complete these tasks, you are ready to start monitoring and configuring your network.

Reference Information

The following sections provide reference information about Prime Infrastructure and its support options.

Ports Used by Prime Infrastructure and Assurance

The below table lists the ports used by Prime Infrastructure and Assurance. These ports must be open in firewalls if you are using these services.

Table 7: Ports Used by Prime Infrastructure and Assurance

Port	Protocol	Direction	Usage
7	TCP/UDP	Server to endpoints	Endpoint discovery via ICMP
20, 21	TCP	Bidirectional server/devices	FTP transfer of files to and from devices
		Server to Cisco.com	FTP download of files from Cisco.com
22	TCP	Server to endpoints	To initiate SSH connection to endpoints during troubleshooting processes
		Client to server	To connect to the Prime Infrastructure server
23	TCP	Server to devices	Telnet communication with devices
25	TCP	Server to SMTP server	SMTP email routing
49	TCP/UDP	Server to TACACS server	Authenticate users using TACACS
53	TCP/UDP	Server to DNS server	DNS
69	UDP	Devices to server	TFTP
80	HTTP	Server to devices	Provisioning of Nexus devices
161	UDP	Server to devices	SNMP polling
162	TCP/UDP	Endpoints to server	SNMP Trap receiver port

Port	Protocol	Direction	Usage
443	TCP	Client to server	Browser access to Prime Infrastructure via HTTPS (enabled by default). This port is also used to check for software updates between the Prime Infrastructure server and cisco.com.
514	UDP	Devices to server	Syslog server
830	TCP	Prime Infrastructure to Device	To open the NETCONF port for communication
1099	TCP/UDP	AAA server to server	RMI registry
1522	TCP/UDP	Primary to secondary server, Secondary to primary server	To configure high availability database connection between the primary and secondary Prime Infrastructure
1645	UDP	Server to RAS	Authenticate Prime Infrastructure users via RADIUS Remote Access Server
1646		RAS to server	
1812		Server to RAS	
1813		RAS to server	
4444	TCP	AAA server to server	RMI server
8078	TCP	PI server to DNA Center Server	Device, Groups, Maps, CMX migration to DNA Center.
8080	TCP	Devices (Cisco Wireless Controllers version 8.6 or higher) to Server	SSL (HTTPS) port for receiving Wireless Client Health Metrics from WLC devices
8082	TCP	Client to server	Health Monitor web interface, Apache/Tomcat JSP engine
8085	TCP	Client to server	Used by the Health Monitor process to check network bandwidth speed between Primary and Secondary servers, when the user executes readiness test under High Availability
8087	TCP	Client to server	Secondary server software update page
9991	UDP	Devices to server	NetFlow data receiver
9992	TCP	Lync server to Prime Infrastructure server	Lync data receiver
10022 to 10041	TCP	Devices to server	Range of ports used for passive FTP file transfers (controller backups, device configurations, report retrieval, and so on)

Port	Protocol	Direction	Usage
11011[6]	TCP	Endpoints to server	Plain text dispatcher port for the Plug and Play Gateway
11012			SSL dispatcher port for the Plug and Play Gateway
11013			Plain text plug and play port
11014			SSL port for the Plug and Play Gateway
20828	TCP	Devices to Coral	Coral accepts TDL based telemetry including AP and client data from devices. (Specific to 16.10 and 16.11 Cisco Catalyst 9800 Wireless Controllers.)
20830	TCP	Devices to Coral	Coral accepts TDL based telemetry including AP and client data from devices. (Specific to 16.12 Cisco Catalyst 9800 Wireless Controllers.)
61617[7]	TCP	Server to endpoints	SSL port for Java Message Service connections

[6] Used when the Plug and Play Gateway is integrated with the Prime Infrastructure server.
[7] Used by the Prime Infrastructure Plug And Play Gateway only.

Remove the Prime Infrastructure Virtual Appliance

Removing Prime Infrastructure using the following method will permanently delete all data on the server, including server settings and local backups. You will be unable to restore your data unless you have a remote backup. For other methods of removal, see *How to Remove Prime Infrastructure* in the latest Cisco Prime Infrastructure Admin Guide .

Procedure

Step 1 In the VMware vSphere client, right-click the Prime Infrastructure virtual appliance.

Step 2 Power off the virtual appliance.

Step 3 Click **Delete from Disk** to remove the Prime Infrastructure virtual appliance.

Navigation and Documentation Reference

This section provides information about navigational paths to access Prime Infrastructure features, and the details of the chapters where the features are covered in the latest Cisco Prime Infrastructure User Guide and the Cisco Prime Infrastructure Administrator Guide.