Cisco APIC-EM Security

Information about Cisco APIC-EM Security

The Cisco APIC-EM requires a multi-layered architecture to support its basic functionality. This multi-layered architecture consists of the following components:

- External network or networks—The external network exists between administrators and applications on one side of the network, and the Grapevine root and clients within an internal network or cloud on the other side. Both administrators and applications access the Grapevine root and clients using this external network.
- Internal network—The internal network consists of both the Grapevine root and clients.
- Device management network—This network consists of the devices that are managed and monitored by the controller. Note that the device management network is essentially the same as the external network described above. This may be physically or logically segmented from the admins or northbound applications.

Important Any inter-communications between the layers and intra-communications within the layers are protected through encryption, authentication, and segmentation.

Note For information about the different services running on the clients within the internal network, see Chapter 3, *Cisco APIC-EM Services*.

External Network Security

The Cisco APIC-EM provides its service over HTTPS and presents its X.509 server public certificate to client communications arriving at any of the external interfaces (eth0, eth1, eth2, etc.). The external clients (for example, northbound REST API consumer applications, devices performing file downloads from the controller, DMVPN certificate renewal, or certificate revocation list (CRL), etc.) may reach the controller via a NAT, proxy gateway, or directly.

The external X.509 certificate that is presented by the controller is one that has been either dynamically generated and self-signed by the controller itself, or one that has been imported (user's X.509 certificate) with a private key into the controller using the GUI. You have the option to either use the a self-signed X.509 certificate from the controller or to import and use your own X.509 certificate and private key. By default, the self-signed X.509 certificate presented to an API request is signed by Grapevine's internal Certificate Authority (CA). This self-signed X.509 certificate may not be recognized and accepted by your host. To proceed with your API request, you must ignore any warning and trust the certificate to proceed.

Note We recommend against using and importing a self-signed certificate into the controller. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended.

Northbound REST API requests from the external network to the Cisco APIC-EM are made secure using the Transport Layer Security (TLS) protocol. Although the controller supports several TLS versions, the default setting for the controller is TLS, version 1.0. You can restrict TLS support to a later and more secure version using the CLI. For additional information, see Configuring the TLS Version Using the CLI, on page 9 .

Related Topics

Configuring the TLS Version Using the CLI, on page 9

Internal Network Security

Several key intra-Grapevine communications using HTTP are sent over SSL using the internal public key infrastructure (PKI). All the internal Grapevine services, database servers, and the Cisco APIC-EM services themselves listen only on the internal network in order to keep these services segmented and secured.

Related Topics

Configuring IPSec Tunneling for Multi-Host Communications, on page 11

Device Management Network Security

Device management network security involves both controller-initiated communications and device-initiated communications.

For controller-initiated communications (discovery or pushing policy to the devices), the Cisco APIC-EM uses the following protocols to access and program network devices:

- SSH version 2
- Telnet
- SNMP versions 2c and 3

Note If supported by the network devices, we strongly recommend using SNMP version v3c with authentication and privacy enabled. The controller does not connect to devices that are SSH version 1. HTTP and HTTPS are not supported for device discovery by the controller.

For device-initiated communications, network devices can use the following protocols to communicate and interact with the controller:

- HTTP
- HTTPS
- SNMP versions 2c

The use of HTTP or HTTPS is not up to the device itself; it is determined by the NB REST API that the device is calling. HTTP is supported for less sensitive communications.

Related Topics

Configuring the TLS Version Using the CLI, on page 9

Information about PKI

The Cisco APIC-EM relies on Public Key Infrastructure (PKI) to provide secure communications. PKI consists of certificate authorities, digital certificates, and public and private keys.

Certificate authorities (CAs) manage certificate requests and issue digital certificates to participating entities such as hosts, network devices, or users. The CAs provide centralized key management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate the hosts, devices and/or individual users. In public key cryptography, such as the RSA encryption system, each entity has a key pair that contains both a private key and a public key. The private key is kept secret and is known only to the owning host, device or user. However, the public key is known to everyone. Anything encrypted with one of the keys can be decrypted with the other. A signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by decrypting the message with the sender's public key. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates link the digital signature to the sender. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The CA that signs the certificate is a third party that the receiver explicitly trusts to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the CA's public key. Typically this process is handled out of band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default.

Supported Cisco APIC-EM PKI Planes

The Cisco APIC-EM maintains two completely separate PKI planes that do not share certificates, keys, or CAs. Each PKI plane secures a particular set of connections:

- **Controller connections**

  The controller's server certificate secures client-initiated connections (communications) to the controller.

  The controller will present its server certificate in response to HTTPS connection requests from NB REST API callers, such as third-party applications that interact with the controller by means of its use of the NB REST API. Additionally, when a router, switch, or other control-plane device initiates an HTTPS connection to the controller to invoke a NB REST API or to download a file (such as a device image, a configuration, etc.) the server presents its certificate to the device that requested the connection.

  Device interactions initiated by the controller, including actions that the controller takes on behalf of a REST caller (for example, discovering devices, managing tags. or pushing policy to devices) do not currently use HTTPS.

  

  Note The security content and discussion in this deployment guide concerns itself solely with this specific PKI plane.

- **Device-to-device DMVPN connections**

  IWAN-managed devices form Dynamic Multipoint VPN (DMVPN) connections between themselves to fulfill the IWAN QoS policy. An embedded private CA in the Cisco APIC-EM provisions the certificates and keys that secure these DMVPN connections. The PKI broker embedded in the Cisco APIC-EM manages these certificates and keys as directed by an admin in the IWAN GUI or a REST caller that uses the pki-broker NB REST API. An external CA cannot manage these certificates and keys.

  Currently, only the IWAN application and the DMVPN connection use the internal CA issued certificates. In future, there may be other services that obtain certificates from the Cisco APIC-EM internal CA.

  

  Note This deployment guide does not discuss the IWAN Dynamic Multipoint VPN (DMVPN) connections. For information about this topic, see the appropriate Cisco IWAN documentation.

Important The internal CA embedded in the Cisco APIC-EM cannot be a sub/intermediate CA to any external CA. Until the Cisco APIC-EM adds such support, these two PKI planes (one for the controller connections and the other for the device-to-device DMVPN connections) remain completely independent of each another. In the current release, the IWAN devices' mutual interaction certificates are managed only by the CA that is embedded in the Cisco APIC-EM. External CAs cannot manage the IWAN-specific certificates that devices present to each other for DMVPN tunnel-creation and related operations.

PKI Device Notifications

The Cisco APIC-EM provides PKI device notifications to assist the user with both troubleshooting and serviceability.

Important The PKI device notifications described in this section are only activated from device-to-device DMVPN connections and not the controller connections.

The following PKI device notifications are available:

- System Notifications—Notifications indicating that user action is required. These notifications are visible from the **Systems Notifications** view that is accessible from the **Global** toolbar in the GUI.
- Audit Log Notifications—Notifications in system logs that are visible using the controller's **Audit Log** GUI.

The following PKI *System* notification types are supported:

- Information
  - New trust point creation
  - New PKCS12 file creation
  - Successful enrollment of a device certificate
  - Successful renewal of a device certificate
  - Revocation of a device certificate
- Warning
  - Partial revocation—Device unreachable or trust point is in use
  - Enrollment delay after 80 percent of a certificate's lifetime
  - Service launch delay
- Critical
  - Certificate Authority handshake failed
  - Enrollment failed
  - Revocation failed

- Renew failed

The following *audit log* notifications are available in the system logs:

- Device enrollment
- Certificate push to the device
- Renewal of a device certificate
- Revocation of a device certificate

Cisco APIC-EM Certificate and Private Key Support

The Cisco APIC-EM supports a PKI certificate management feature that is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents called certificate authorities (CAs). The Cisco APIC-EM uses the PKI certificate management feature to import, store, and manage an X.509 certificate from well-known CAs. The imported certificate becomes an identity certificate for the controller itself, and the controller presents this certificate to its clients for authentication. The clients are the NB API applications and network devices.

The Cisco APIC-EM can import the following files (in either PEM or PKCS file format) using the controller's GUI:

- X.509 certificate
- Private key

Note For the private key, Cisco APIC-EM supports the importation of RSA keys. You should not import DSA, DH, ECDH, and ECDSA key types; they are not supported. You should also keep the private key secure in your own key management system.

Prior to import, you must obtain a valid X.509 certificate and private key from a well-known, certificate authority (CA) or create your own self-signed certificate. After import, the security functionality based upon the X.509 certificate and private key is automatically activated. The Cisco APIC-EM presents the certificate to any device or application that requests them. Both the northbound API applications and network devices can use these credentials to establish a trust relationship with the controller.

In an IWAN configuration and for the Network PnP functionality, an additional procedure involving a PKI trustpool is used to ensure trust between devices within the network. See the following *Cisco APIC-EM Trustpool Support* section for information about this procedure.

Note We recommend against using and importing a self-signed certificate into the controller. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended. Additionally, you must replace the self-signed certificate (installed in the Cisco APIC-EM by default) with a certificate that is signed by a well-known certificate authority for the Network PnP functionality to work properly.

The Cisco APIC-EM supports only one imported X.509 certificate and private key at a time. When you import a second certificate and private key, it overwrites the first (existing) imported certificate and private key values.

Note If the external IP address changes for your controller for any reason, then you need to re-import a new certificate with the changed or new IP address.

Related Topics

Importing a Certificate

Cisco APIC-EM Certificate Chain Support

The Cisco APIC-EM is able to import certificates and private keys into the controller through its GUI. The Cisco APIC-EM also supports the importation of subordinate certificates (intermediate certificates) from a subordinate Certificate Authority (CA) through its GUI.

If there are subordinate certificates involved in the certificate chain leading to the certificate that is imported into the controller (controller certificate), then both the subordinate certificates as well as the root certificate of these subordinate CAs must be appended together into a single file to be imported. When appending these certificates, you must append them in the same order as the actual chain of certification.

For example, assume that a well-known and trusted CA with a root certificate (CA root) signed an intermediate CA certificate (CA1). Next, assume that this certificate, CA1 signs another intermediate CA certificate (CA2). Finally, assume that the CA certificate (CA2) was the CA that signed the controller certificate (Controller_Certificate). In this example, the PEM file that needs to be created and imported into the controller should have the following order from the top (beginning) of the file to the bottom of the file (end):

1. Controller_Certificate (top of file)
2. CA2 certificate
3. CA1 certificate

The requirement to append the root and subordinate certificates to the controller certificate to create a single file only applies to a PEM file. The requirement for appending a root and intermediate certificates to a root certificate for import is not required for a PKCS file.

Related Topics

Importing a Certificate

Cisco APIC-EM Trustpool Support

The Cisco APIC-EM and Cisco IOS devices support a special PKI certificate store known as the trustpool. The trustpool holds X.509 certificates that identify trusted certificate authorities (CAs). The Cisco APIC-EM and the devices in the network use the trustpool bundle to manage trust relationships with each other and with these CAs. The controller manages this PKI certificate store and has the ability to update it through its GUI when certificates in the pool are due to expire, are reissued, or must be changed for other reasons.

Note The Cisco APIC-EM also uses the trustpool functionality to determine whether any certificate file that is uploaded via its GUI is a valid CA signed certificate or not.

The Cisco APIC-EM contains a pre-installed, default, Cisco-signed trustpool bundle named ios.p7b. This trustpool bundle is trusted by supported Cisco network devices natively, since it is signed with a Cisco digital signing certificate. This trustpool bundle is critical for the Cisco network devices to establish trust with services and applications that are genuine. This Cisco PKI trustpool bundle file is available on the Cisco website (Cisco InfoSec).

The link is located at:http://www.cisco.com/security/pki/

For the controller's Network PnP functionality, the supported Cisco devices that are being managed and monitored by the controller need to import this file. When the supported Cisco devices first boot-up, they contact the controller to import this file.

Note At times, you may need to update this trustpool bundle to a newer version due to certificates in the trustpool expiring, being reissued, or for other reasons. Whenever the trustpool bundle that exists on the controller needs to be updated, you can update it by using the controller's GUI. The controller can access the Cisco cloud (where the Cisco approved trustpool bundles are located) and download the latest trustpool bundle. After download, the controller then overwrites the current, older trustpool bundle file. As a practice, you may want to update the trustpool bundle before a new certificate from a CA is to be imported using the **Certificate** window or the **Proxy Gateway Certificate** window, or whenever the **Update** button is active and not grayed out.

The Cisco APIC-EM trustpool management feature operates in the following way:

1. You boot-up the Cisco devices within your network that supports the Network PnP functionality.

   Note that **not** all Cisco devices support the Network PnP functionality. See the *Release Notes for Cisco Network Plug and Play* for a list of the supported Cisco devices.

2. As part of initial PnP flow, these supported Cisco devices download a trustpool bundle directly from the Cisco APIC-EM using HTTP.
3. The Cisco devices are now ready to interact with the Cisco APIC-EM to obtain further device configuration and provisioning per the Network PnP traffic flows.

Important If an HTTP proxy gateway exists between the controller and these Cisco devices, then perform an additional procedure to import the proxy gateway certificate into the controller. See Importing a Proxy Gateway Certificate.

Related Topics

Importing a Trustpool Bundle

Security and Cisco Network Plug and Play

With the Cisco Network Plug and Play (PnP) application, the Cisco APIC-EM responds to HTTPS requests from supported Cisco network devices and permits these devices to download and install an image and desired configuration. Before a device can download these files from the controller, the initial interaction between the controller and device involves the establishment of a trust relationship.

At first interaction with a PnP enabled device, that PnP enabled device is provisioned by the controller with trust information that includes a CA root certificates bundle or at the least the certificate of the CA that issued the server side certificate. Note that in latter case, the CA may or may not be a well known CA.

In certain Cisco Network Plug and Play scenarios, your network configuration may have a proxy gateway present between the controller and PnP enabled devices. For example, in an IWAN deployment a branch router may communicate with the Cisco APIC-EM through a proxy gateway at the DMZ at initial provisioning. Depending upon whether there is a proxy gateway present or not, the trust information provided by the controller at the initial transaction with the devices may correspond to the proxy gateway's or to the controller's certificate issuer (if the corresponding server certificates are not valid CA signed). On the other hand, in either proxy or non-proxy cases, if the certificate is a simple self-signed certificate, then that certificate will be downloaded by the device into its trust store.

Note Using a self-signed certificate for either the Cisco APIC-EM or the proxy gateway is strongly discouraged. We strongly recommend using a publicly verifiable CA issued certificate to be installed on the controller, as well as the proxy gateway if one is present.

With a valid CA issued certificate for the controller or the proxy gateway (if present), the PnP enabled devices can download the trustpool bundle (ios.p7b) containing all the well known CA root certificates. This permits the devices to establish secure connections to the controller or to the proxy gateway for further provisioning and operation of those devices. If such a certificate is not a valid CA issued or self-signed, then the devices will have to download the issuing CA's or self-signed certificate to proceed further with a secure connection to the controller or a proxy gateway in front of the controller. The Cisco APIC-EM facilitates automatic downloads of the relevant trusted certificates on the devices, depending on the nature of the certificate installed on it. However; when a proxy gateway is present, the controller provides a provisioning GUI to facilitate similar pre-provisioning.

Related Topics

Importing a Proxy Gateway Certificate

Configuring the TLS Version Using the CLI

Northbound REST API requests from the external network to the Cisco APIC-EM (from northbound REST API based apps, browsers, and network devices connecting to the controller using HTTPS) are made secure using the Transport Layer Security protocol (TLS). The Cisco APIC-EM supports TLS versions 1.0, 1.1, and 1.2.

The minimum TLS version that a client (either a northbound application client such as the controller GUI browser or a network device) can communicate with the controller by default is TLS 1.0. If your network device IOS/XE versions can support a higher version than TLS 1.0, then it is strongly recommended to configure the minimum TLS version of the controller to the higher version (be sure that all of your network devices under Cisco APIC-EM control can support this higher TLS version).

Note Any versions lower than TLS 1.0 (such as SSLv3 and SSLv2) are not supported by Cisco APIC-EM.

Important With the controller TLS version set to 1.2, a client initiating a TLS version 1.0 or 1.1 connection will be rejected and any communications from this client will fail. With the controller TLS version set to 1.0, a client initiating a TLS version 1.1 or 1.2 connection will be permitted.

You configure the TLS version for the controller by logging into the host (physical or virtual) and using the CLI.

Note This security feature applies only to port 443 on the Cisco APIC-EM .

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have grapevine SSH access privileges to perform this procedure.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **grape config display** command at the prompt to display the default TLS minimum version.

```
$ grape config display

PROPERTY                          VALUE
------------------------------------------------------------------------
client_grow_timeout               150
client_heartbeat_timeout          120
client_idle_timeout               60
enable_policy                     True
enable_secure_tunnel              True
enable_service_rollback           False
host_cpu_threshold                0.9
host_datastore_threshold          1.0
host_heartbeat_timeout            120
host_memory_threshold             0.00999999977648
https_proxy
https_proxy_password
https_proxy_username
load_multiplier                   1.0
max_spare_capacity                1
policy_startup_delay              120
tls_minimum                       1_0

(grapevine)
```

Step 4 Enter the **grape config update tls_minimum 1_2** command at the prompt to update to TLS version 1.2

```
$ grape config update tls_minimum 1_2
```

```
Config updated successfully

(grapevine)
```

Step 5 Enter the **grape config display** command at the prompt a second time to view the new TLS minimum version.

```
$ grape config display

PROPERTY                          VALUE
------------------------------------------------------------------------
client_grow_timeout               150
client_heartbeat_timeout          120
client_idle_timeout               60
enable_policy                     True
enable_secure_tunnel              True
enable_service_rollback           False
host_cpu_threshold                0.9
host_datastore_threshold          1.0
host_heartbeat_timeout            120
host_memory_threshold             0.00999999977648
https_proxy
https_proxy_password
https_proxy_username
load_multiplier                   1.0
max_spare_capacity                1
policy_startup_delay              120
tls_minimum                       1_2

(grapevine)
```

The TLS minimum version should display *1_2*, which indicates the TLS 1.2 version.

Related Topics

External Network Security, on page 2

Device Management Network Security , on page 2

Configuring IPSec Tunneling for Multi-Host Communications

The default tunneling protocol used for inter-host communications in a multi-host cluster is Generic Routing Encapsulation (GRE). Communications between the hosts in a multi-host cluster can be made more secure using Internet Protocol Security (IPsec). You can enable secure tunneling with IPSec for the Cisco APIC-EM using the configuration wizard, as described in this procedure.

Important If you are upgrading from a prior Cisco APIC-EM release version, to release version 1.2.x, then follow the upgrade procedure as described in the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.2.0.x*. This procedure describes the process for configuring IPSec tunneling on a fresh installed 1.2.x multi-host cluster.

Follow the steps described below to enhance security for communications between the hosts. The steps are organized as follow:

1. Break up or disassemble your multi-host cluster (steps 1-5).
2. Enable IPSec tunneling on the last host that was in your cluster (steps 6-10).
3. Reassembly your multi-host cluster around that host where you enabled IPSec tunneling. (steps 10-20).

Note You should not enable or disable the secure tunnel mode (IPSec tunneling) while the Cisco APIC-EM is in a multi-host cluster. The configuration wizard does not support such a change while in a multi-host cluster.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have grapevine SSH access privileges to perform this procedure.

Step 1 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 2 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 4 A message appears with an option to **[proceed]** and remove this host from the cluster.
Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from the cluster.
At the end of this process, this host is removed from the cluster.

Step 5 Repeat the above steps (steps 1-4) on a second host in the cluster.

Note You must repeat the above steps on each host in your cluster, until you have broken up the multi-host cluster.

Important Make a note of the final host in the cluster that you have just broken up or disassembled. You must perform the next steps (enabling IPSec tunneling) on that specific host. For example, if you have 3 hosts in a cluster (A, B , C) and you first remove host A, then remove host B, then you must enable IPSec on host C.

Step 6 Using a Secure Shell (SSH) client, log into the last host in your cluster and run the **config_wizard** command.

```
$ config_wizard
```

Step 7 Review the current configuration values in the configuration wizard and click **next>>**, until you access the **INTER-HOST COMMUNICATION** screen.

Step 8 Configure IPSec tunneling for communications between the hosts in a multi-host cluster by selecting *yes*.

The default tunneling protocol used for communications between the hosts in a multi-host cluster is Generic Routing Encapsulation (GRE). By entering 'yes', you are configuring IPSec tunneling with this step.

Step 9 Click **next>>** until the last step of the configuration wizard process is reached.

Step 10 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM deployment.
At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Next, proceed to log into the other hosts previously in your multi-host cluster and use the configuration wizard to reassemble the cluster (with IPSec tunneling configured between the hosts).

Step 11 Using a Secure Shell (SSH) client, log into one of the other hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 12 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 13 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option.

Note Joining this other (second) host to the host with the enabled IPSec tunneling, automatically configures IPSec tunneling on this other (second) host.

Step 14 Proceed to recreate the cluster using the configuration wizard.
For additional information about this step and process, see Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard.

Step 15 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

Step 16 Using a Secure Shell (SSH) client, log into the third host and use the configuration wizard to join the new multi-host cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 17 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 18 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Add this host to an existing APIC-EM cluster** option.

Note Adding this host to the new multi-host cluster with the enabled IPSec tunneling, automatically configures IPSec tunneling on this host.

Step 19 Proceed to add this host to the cluster using the configuration wizard.
For additional information about this step and process, see Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard..

Step 20 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

At the end of this step, you have updated your cluster and configured IPSec tunneling. Repeat the above steps to add any additional hosts to your multi-host cluster.

Related Topics

Internal Network Security, on page 2

Password Requirements

The Cisco APIC-EM password policy governs password values in logins to the controller GUI, SSH logins to the Grapevine root, northbound API requests, and logins to the Grapevine console for troubleshooting. The Cisco APIC-EM rejects a password that does not conform to the password policy. If a password is rejected, the controller provides an error message that describes the reason for the rejection.

A new or changed password must meet the following criteria:

- Eight character minimum length.
- Does NOT contain a tab or a line break.
- Does contain characters from at least three of the following categories:
  - Uppercase alphabet
  - Lowercase alphabet
  - Numeral
  - Special characters

    Special characters include the space character or any of the following characters or character combinations:

```
! @ # $ % ^ & * ( ) - =  + _ { } [ ] \\ | ; : " ' , < . > ? /
:: #! ./ ;; >> << () **
```

For example, `Splunge!` is a valid password because it meets the eight-character minimum length, contains at least one uppercase alphabetic character, contains at least one lowercase alphabetic character, and contains at least one special character (`!`).

Related Topics

Configuring Password Policies

Cisco APIC-EM Ports Reference

The following tables list the Cisco APIC-EM ports that permit incoming traffic, as well as the Cisco APIC-EM ports that are used for outgoing traffic. You should ensure that these ports on the controller are open for both incoming and outgoing traffic flows.

The following table lists Cisco APIC-EM ports that permit *incoming* traffic into the controller.

Note Ensure proper protections in your network for accessing ports 22 and 14141.

Table 1: Cisco APIC-EM Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
67	bootps	UDP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443 [1]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP (Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP
14141	Grapevine console	TCP
16026	SCEP	TCP

1 You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see Configuring the TLS Version Using the CLI, on page 9

The following table lists Cisco APIC-EM ports that are used for *outgoing* traffic from the controller.

Table 2: Cisco APIC-EM Outgoing Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH (to the network devices)	TCP
23	Telnet (to the network devices)	TCP
53	DNS	UDP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
80	Port 80 may be used for an outgoing proxy configuration. Additionally, other common ports such as 8080 may also be used when a proxy is being configured by the Cisco APIC-EM configuration wizard (if a proxy is already in use for your network). **Note** To access Cisco supported certificates and trust pools, you can configure your network to allow for outgoing IP traffic from the controller to Cisco addresses at the following URL: http://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP agent	UDP
443 [2]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP ((Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP

2 You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see Configuring the TLS Version Using the CLI, on page 9