Security

This chapter contains the following sections:

RADIUS Client

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The device can be configured to be a RADIUS client that can use a RADIUS server to provide centralized security, and as a RADIUS server. An organization can use the device as establish a Remote Authorization Dial-In User Service (RADIUS) server to provide centralized 802.1X or MAC-based network access control for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

Use RADIUS in network environments that require access security. To set the RADIUS server parameters, follow these steps:

Step 1 Click **Security** > **RADIUS Client**.

Step 2 Enter the default RADIUS parameters if required. Values entered in the Default Parameters are applied to all servers. If a value is not entered for a specific server (in the Add RADIUS Server page) the device uses the values in these fields.

- Retries—Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.
- Timeout for Reply—Enter the number of seconds that the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
- Dead Time—Enter the number of minutes that elapse before a non-responsive RADIUS server is bypassed for service requests. If the value is 0, the server is not bypassed.
- Key String—Enter the default key string used for authenticating and encrypting between the device and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. The key can be entered in Encrypted or Plaintext form. If you do not have an encrypted key string (from another device), enter the key string in plaintext mode and click Apply. The encrypted key string is generated and displayed.

This overrides the default key string if one has been defined.

- Source IPv4 Interface—Select the device IPv4 source interface to be used in messages for communication with the RADIUS server.
- Source IPv6 Interface—Select the device IPv6 source interface to be used in messages for communication with the RADIUS server.

Note If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 3 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

Step 4 To add a RADIUS server, click **Add**.

Step 5 Enter the values in the fields for each RADIUS server.

- Server Definition—Select whether to specify the RADIUS server by IP address or name.
- IP Version—Select the version of the IP address of the RADIUS server.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list. •
- Server IP Address/Name—Enter the RADIUS server by IP address or name.
- Priority—Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority RADIUS server first. Zero is the highest priority.
- Key String—Enter the key string used for authenticating and encrypting communication between the device and the RADIUS server. This key must match the key configured on the RADIUS server. It can be entered in Encrypted or Plaintext format. If Use Default is selected, the device attempts to authenticate to the RADIUS server by using the default Key String.

- Timeout for Reply—Select User Defined and enter the number of seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server if the maximum number of retries made. If Use Default is selected, the device uses the default timeout value.
- Authentication Port—Enter the UDP port number of the RADIUS server port for authentication requests
- Retries—Select User Defined and enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. If Use Default is selected, the device uses the default value for the number of retries.
- Dead Time—Select User Defined and enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. If Use Default is selected, the device uses the default value for the dead time. If you enter 0 minutes, there is no dead time.
- Usage Type—Enter the RADIUS server authentication type. The options are:
  - Login—RADIUS server is used for authenticating users that ask to administer the device.
  - 802.1x—RADIUS server is used for 802.1x authentication.
  - All—RADIUS server is used for authenticating user that ask to administer the device and for 802.1X authentication.

Step 6 Click **Apply**. The RADIUS server definition is added to the Running Configuration file of the device.

Step 7 To display sensitive data in plaintext form on the page, click **Display Sensitive Data As Plaintext**.

Dynamic Authorization Server

Change of Authorization (CoA) is an extension to the RADIUS protocol, allowing dynamic changes to an AAA or dot1x user session. This includes support for disconnecting users and changing authorizations applicable to a user session. The device supports the following CoA actions:

- Disconnect Session
- Disable host port CoA command
- Bounce host port CoA command
- Reauthenticate host CoA command

Perform the following steps to enable the device as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. Change of Authorization (CoA) is an extension to the RADIUS protocol, allowing dynamic changes to an AAA or dot1x user session. This includes support for disconnecting users and changing authorizations applicable to a user session.

Step 1 Click **Security** > **Dynamic Authorization Server**>

Step 2 Configure the following settings:

Setting	Description
Enforce Server Key Match	Check **Enable** to enforce server key match. If this control is disabled then the RADIUS exchange with the CoA client will succeed even the key configured on the device and on the CoA client do not match.
Enforce Timestamp on Rx	Check **Enable** to enforce timestamp on received Packet of Disconnect (POD) Request or Change of Authorization (CoA). If these packets do not include a time stamp they will be discarded.
Handle Disable Port Commands	Check **Enable** to enable the handle of CoA disable port command. When unchecked the device will ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions.
Handle Bounce Port Commands	Check **Enable** to enable the handle of CoA bounce port command. When unchecked the device will ignore a RADIUS server bounce port command that causes to link flap on an authentication port, which causes DHCP renegotiation from one or more hosts connected to this port.
Default Server Key MD5	Defines the Shared key between the device and the CoA client. Select one of the following: • None • Keep existing default key • User Defined (Encrypted) • User Defined (Plaintext)
UDP Port	Enter a value to configure the UDP port for CoA request (Range 0 - 59999, Default: 1700).
Domain Stripping	Configures username domain options for the CoA application. Select from one of the following options: • None - No domain stripping • Left to Right - The left-to-right keyword terminates the string at the first delimiter going from left-to-right. • Right to Left - The right-to-left keyword terminates the string at the first delimiter going from right to left
Domain Delimiter	The delimiter field specifies the domain delimiter. One of the following options can be selected for the character argument: @ , / , $, % , \ , # , or -.

Step 3 The Client table defines a per CoA client MD5 server key for a specific CoA client(s). The per client key overrides the key defined in the Default Server Key MD5 setting. If a key wasn't defined for a certain CoA client, then the client will use the Default Server Key MD5. To add a key for a certain CoA client, click **Add**. in the popup window, configure the following: and configure the following:

- IP Address - The IPv4 or IPv6 address of the CoA client
- Server Key - Select one of the following:

- User default key - in this case the default server key will be used.
- User Defined (Encrypted) - enter the key in the encrypted format.
- User Defined (Plaintext) - enter the key in the plaintext format.

Step 4 Click **Apply** to apply the settings.

Login Settings

The default username/password is **cisco/cisco**. The first time that you log in with the default username and password, you're required to enter a new password. Password complexity is enabled by default. If the password that you choose isn't complex enough, then you will be prompted to create another password.

Step 1 Click **Security > Login Settings** .

Step 2 Next, configure the following:

Option	Description
Password Aging	Check **Enable** to enable the password aging. It is disabled by default.
Password Aging Time	Enter the number of days. (Range: 1 - 365, Default: 180) **Note** A warning message will appear 10 days prior to the password expiration date providing the option to change the password. User can ignore the warning and continue to use the existing password until the actual expiration date.
Recent Password Prevention	Check **Enable** to enable this feature. It is disabled by default.
Password History Count	Defines the number for a recent password prevention. range is 1- 24 and default is 12.
Minimal Password Length	Enter the number of character for the password. (Range: 8-64, Default: 8)
Allowed Character Repetition	A character cannot be repeated consecutively. Enter a number for the allowed character repetition. (Range: 1- 16, Default: 3)
Minimal Number of Character Classes:	Enter a number for the minimal number of character classes. (Range: 1- 4, Default: 3)

Note The password complexity rules are as follows:

- Minimal password length is 8 characters by default. Passwords are configurable with a range of 8-64.
- Minimum number of character classes: The number of different character classes that must be included in the password (classes are: uppercase letter, lowercase letter, number and special character). The minimum number is 3 by default and is configurable to 0-4 (0 and 1 are functionally identical).
- Any password established or altered by the user (hence "Secret") is compared to a list of common passwords. If the secret contains a word from the list, the user will receive the following error message and will need to re-enter an alternative password: "Password rejected- Passwords must not match words in the dictionary, and must not contain commonly used passwords".
- Context specific words (project and vendor name) – The password MUST NOT contain the username or the words “cisco” , "catalyst" or derivatives of such. This restriction includes these words reversed or in any case. Restriction also includes letters that are replaced with other characters, as follows: "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e", is not permitted. For example, C!$c0678! is not permitted.
- Known passwords are not allowed as passwords

Definition for Known Password

When a user attempts to configure a new password, it is compared against the list of commonly used passwords. If new password matches or begins with one of the passwords in the common password list. The comparison to passwords on the list is case insensitive.

If the new password does not comply to the above requirement, the user configuration is rejected and the user will need to configure a different password.

Definition for Sequential Characters

The password MUST NOT contain more than a 2 sequential characters or numbers. The limitation applies to sequential letters in any case (e.g. AbC or aBC).

Examples for prohibited passwords: “eFg152!$”, “aztb567%”.

If the password does not comply to these rules the configuration will be rejected and the user will need to configure a new password.

Login Lockdown

If the address of a device is known, a malicious user may attempt to perform a dictionary attack. A dictionary attack is an automated process to attempt to login by attempting thousands, or even millions, of credentials. The purpose of a dictionary attack is to actually gain management access to the device.

To prevent these attacks the device can be configured to limit the amount of login attempts allowed within a specific time range and by defining a quiet mode period following a specified number of failed attempts. If the specified number of connection attempts fails (attempt tries) within a specified time (within seconds), the device will not accept any additional login attempts for a specified period of time (block-for seconds). This can also occur when the user forgets his login credentials and tries to login several times resulting in login failure.

Note Following a specified number of failed login attempts over a specified time period, the device will enter into quiet mode. The device will not accept any more connection requests during the quiet mode time, including telnet, SSH, SNMP, HTTP, or HTTPS. The device will restart accepting connection requests once the quiet mode period has ended. The start and conclusion of the quiet mode time will be indicated by a Syslog message.

The number of failed attempts should be counted throughout a period of time that is measured from each failed attempt. Failed attempts are not counted during the quiet period. When the quiet period expires, the count of failed attempts resumes. A quiet period can be ended before the timer expires by disabling the functionality.

Step 1 In the Login Response Delay, check **Enable** to enable the login response delay.

Step 2 Next, configure the following:

Option	Description
Response Delay Period	Enter a number in seconds to set the response delay period. (Range: 1- 10, Default: 1)
Quiet Period Enforcement	Check **Enable** to enforce quite period.
Quiet Period Length	Enter the number of seconds to set the quiet period length. (Range: 1- 65535, Default: 300)
Triggering Attempts	Enter the number of triggering attempts. (Range: 1- 100, Default: 4)
Triggering Interval	Enter the number in seconds for triggering interval. (Range: 1- 3600, Default: 60)
Quiet Period Access Profiles, on page 9. **Note** This link navigates to the Security → Management Access Method → Access Profiles page.	Console Only is the default setting. **Note** This drop down contains an option for every existing access profile.

Login Protection Status

The Login Protection Status page will track and display any attempted attacks or login failures. (It will not distinguish if the login failure is a user who forgot his credentials or an actual attack). Click the **Refresh** button to refresh the data.

To view the settings for the Login Protection Status, navigate to **Security > Login Protection Status.**

- Quiet Mode Status- Can have either an active or inactive status.
- Login Failures in the Last 3600 Seconds- Displays the number of login failures during the time lapse defined by the "Quiet Period Length" Parameter. The "Quiet Period Length" is a value in seconds configured in the **Security > Login Settings** page.

In the Login Failure Table, the following will be displayed:

- Username- the name of the user
- IP Address- the IP address of the user
- Service- the service being used. This can be either HTTP, HTTPS, Telnet, SSH or SNMP.
- Count- the number of attempted login failures.
- Most Recent Attempt Time- the most recent time that a failed login was attempted.

Management Access Method

This section describes access rules for various management methods.

Access profiles determine how to authenticate and authorize users accessing the device through various access methods. Access Profiles can limit management access from specific sources.

Only users who pass both the active access profile and the management access authentication methods are given management access to the device.

There can only be a single access profile active on the device at one time.

Access profiles consist of one or more rules. The rules are executed in order of their priority within the access profile (top to bottom).

Rules are composed of filters that include the following elements:

- Access Methods-Methods for accessing and managing the device:
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - All of the above
- Action-Permit or deny access to an interface or source address.
- Interface-Which ports, LAGs, or VLANs are permitted to access or are denied access to the web-based configuration utility.
- Source IP Address-IP addresses or subnets. Access to management methods might differ among user groups. For example, one user group might be able to access the device module only by using an HTTPS session, while another user group might be able to access the device module by using both HTTPS and Telnet sessions.

Access Profiles

The Access Profiles page displays the access profiles that are defined and enables selecting one access profile to be the active one.

When a user attempts to access the device through an access method, the device looks to see if the active access profile explicitly permits management access to the device through this method. If no match is found, access is denied.

When an attempt to access the device is in violation of the active access profile, the device generates a SYSLOG message to alert the system administrator of the attempt.

If a console-only access profile has been activated, the only way to deactivate it's through a direct connection from the management station to the physical console port on the device.

For more information, see Profile Rules, on page 10.

Use the Access Profiles page to create an access profile and to add its first rule. If the access profile only contains a single rule, you're finished. To add more rules to the profile, use the Profile Rules page.

Step 1 Click **Security** > **Mgmt Access Method** > **Access Profiles**.

Step 2 To change the active access profile, select a profile from the Active Access Profile drop down menu and click **Apply**.

Step 3 A pop-up will appear asking you to confirm the Active Access Profile change. Click **OK** to confirm or click **Cancel** to cancel.

Step 4 Click **Add** to open the Add Access Profile page. The page allows you to configure a new profile and one rule.

Step 5 Enter the Access Profile Name. This name can contain up to 32 characters.

Step 6 Enter the parameters.

- Rule Priority—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. The highest priority is '1'.
- Management Method—Select the management method for which the rule is defined. The options are:
  - All—Assigns all management methods to the rule
  - Telnet—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
  - Secure Telnet (SSH)—Users requesting access to the device that meets the SSH access profile criteria, are permitted or denied access.
  - HTTP— Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
  - Secure HTTP (HTTPS)—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
  - SNMP—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- Action—Select the action attached to the rule. The options are:
  - Permit—Permits access to the device if the user matches the settings in the profile.

- Deny—Denies access to the device if the user matches the settings in the profile

- Applies to Interface—Select the interface attached to the rule. The options are:
  - All—Applies to all ports, VLANs, and LAGs
  - User Defined—Applies to selected interface.
- Interface—Enter the interface number if User Defined was selected.
- Applies to Source IP Address—Select the type of source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork. Select one of the following values:
  - All—Applies to all types of IP addresses
  - User Defined—Applies to only those types of IP addresses defined in the fields.
- IP Version—Enter the version of the source IP address: Version 6 or Version 4.
- IP Address—Enter the source IP address.
- Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Network Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix Length—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

Step 7 Click **Apply**. The access profile is written to the Running Configuration file. You can now select this access profile as the active access profile.

Profile Rules

Access profiles can contain up to 128 rules to determine who is permitted to manage and access the device, and the access methods that may be used. Each rule in an access profile contains an action and criteria (one or more parameters) to match. Each rule has a priority; rules with the lowest priority are checked first. If the incoming packet matches a rule, the action associated with the rule is performed. If no matching rule is found within the active access profile, the packet is dropped.

For example, you can limit access to the device from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the device can still be managed and has gained another layer of security.

To add profile rules to an access profile, complete the following steps:

Step 1 Click **Security** > **Mgmt Access Method** > **Profile Rules**.

Step 2 Select the Filter field, and an access profile. Click **Go**.

The selected access profile appears in the Profile Rule Table.

Step 3 Click **Add** to add a rule.

Step 4 Enter the parameters.

- Access Profile Name—Select an access profile.
- Rule Priority—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.
- Management Method—Select the management method for which the rule is defined. The options are:
  - All—Assigns all management methods to the rule
  - Telnet—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
  - Secure Telnet (SSH)—Users requesting access to the device that meets the Telnet access profile criteria, are permitted or denied access.
  - HTTP—Assigns HTTP access to the rule Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
  - Secure HTTP (HTTPS)—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
  - SNMP—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- Action—Select one of the following options.
  - Permit—Allow device access to users coming from the interface and IP source defined in this rule.
  - Deny—Deny device access to users coming from the interface and IP source defined in this rule.
- Applies to Interface—Select the interface attached to the rule. The options are:
  - All—Applies to all ports, VLANs, and LAGs
  - User Defined—Applies only to the port, VLAN, or LAG selected.
- Interface—Enter the interface number if the User Defined option is selected for the field above.
- Applies to Source IP Address—Select the type of source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork. Select one of the following values:
  - All—Applies to all types of IP addresses
  - User Defined—Applies to only those types of IP addresses defined in the fields.
- IP Version—Select the supported IP version of the source address: IPv6 or IPv4.
- IP Address—Enter the source IP address.
- Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Network Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix Length—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

Step 5 Click **Apply** and the rule is added to the access profile.

Management Access Authentication

You can assign authentication methods to the various management access methods, such as SSH, Telnet, HTTP, and HTTPS. The authentication can be performed locally or on a server.

If authorization is enabled, both the identity and read/write privileges of the user are verified. If authorization isn't enabled, only the identity of the user is verified.

The authorization/authentication method used is determined by the order that the authentication methods are selected. If the first authentication method isn't available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and all configured RADIUS servers are queried in priority order and don't reply, the user is authorized/authenticated locally.

If authorization is enabled, and an authentication method fails or the user has insufficient privilege level, the user is denied access to the device. In other words, if authentication fails for an authentication method, the device stops the authentication attempt; it doesn't continue and doesn't attempt to use the next authentication method.

Similarly, if authorization isn't enabled, and authentication fails for a method, the device stops the authentication attempt.

To define authentication methods for an access method:

Step 1 Click **Security** > **Management Access Authentication**.

Step 2 Enter the Application (type) of the management access method.

Step 3 Select **Authorization** to enable both authentication and authorization of the user by the list of methods described below. If the field is not selected, only authentication is performed. If Authorization is enabled, the read/write privileges of users are checked. This privilege level is set in the User Accounts page.

Step 4 Use the arrows to move the authentication method between the Optional Methods column and the Selected Methods column. The first method selected is the first method that is used.

- RADIUS—User is authorized/authenticated on a RADIUS server. You must have configured one or more RADIUS servers. For the RADIUS server to grant access to the web-based configuration utility, the RADIUS server must return RADIUS Attribute "Service-Type 6" value "Administrative".
- None—User is allowed to access the device without authorization/authentication.
- Local—Username and password are checked against the data stored on the local device. These username and password pairs are defined in the User Accounts page.

  Note The Local or None authentication method must always be selected last. All authentication methods selected after Local or None are ignored.

Step 5 Click **Apply**. The selected authentication methods are associated with the access method.

Secure Sensitive Data Management

SSD protects sensitive data on a device, such as passwords and keys, permits and denies access to sensitive data encrypted and in plain text based on user credentials and SSD rules, and protects configuration files containing sensitive data from being tampered with.

In addition, SSD enables the secure backup and sharing of configuration files containing sensitive data.

SSD provides users with the flexibility to configure the desired level of protection on their sensitive data; from no protection with sensitive data in plaintext, minimum protection with encryption based on the default passphrase, and better protection with encryption based on user-defined passphrase.

SSD grants read permission to sensitive data only to authenticated and authorized users, and according to SSD rules. A device authenticates and authorizes management access to users through the user authentication process.

Whether or not SSD is used, it is recommended that the administrator secure the authentication process by using the local authentication database, and/or secure the communication to the external authentication servers used in the user authentication process.

In summary, SSD protects sensitive data on a device with SSD rules, SSD properties, and user authentication. And SSD rules, SSD properties, and user authentication configurations of the device are themselves sensitive data protected by SSD.

SSD Properties

SSD properties are a set of parameters that, in conjunction with the SSD rules, define and control the SSD environment of a device. The SSD environment consists of these properties:

- Controlling how the sensitive data is encrypted.
- Controlling the strength of security on configuration files.
- Controlling how the sensitive data is viewed within the current session.

To configure the SSD properties, follow these steps:

Step 1 Click **Security** > **Secure Sensitive Data Management** > **Properties**.

The following field appears:

- Current Local Passphrase Type—Displays whether the default passphrase or a user-defined passphrase is currently being used.

Step 2 In the Configuration File Passphrase Control—Select an option from the following:

- Unrestricted (default)—The device includes its passphrase when creating a configuration file. This enables any device accepting the configuration file to learn the passphrase from the file.
- Restricted—The device restricts its passphrase from being exported into a configuration file. Restricted mode protects the encrypted sensitive data in a configuration file from devices that do not have the passphrase. This mode should be used when a user does not want to expose the passphrase in a configuration file.

Step 3 Next, select to enable the Configuration File Integrity Control.

Step 4 Select a Read Mode for the current session

- Plaintext —Users are permitted to access sensitive data in plaintext only. Users will also have read and write permission to SSD parameters.
- Encrypted —Users are permitted to access sensitive data as encrypted only.

Step 5 Click **Change Local Passphrase**, and enter a new Local Passphrase:

- Default—Use the devices default passphrase.
- User Defined (Plaintext)—Enter a new passphrase.
- Confirm Passphrase—Confirm the new passphrase.

Step 6 Click **Apply**. The settings are saved to the Running Configuration file.

SSD Rules

Only users with SSD read permission of Plaintext-only or Both are allowed to set SSD rules.

To configure SSD rules, follow these steps:

Step 1 Click **Security** > **Secure Sensitive Data Management** > **SSD Rules**.

The currently-defined rules are displayed. The Rule Type field indicates whether the rule is a user-defined one or a default rule.

Step 2 To add a new rule, click **Add**. Enter the following fields:

- User—This defines the user(s) to which the rule applies: Select one of the following options:
  - Specific User—Select and enter the specific user name to which this rule applies (this user does not necessarily have to be defined).
  - Default User (cisco)—Indicates that this rule applies to the default user.
  - Level 15—Indicates that this rule applies to all users with privilege level 15.
  - All—Indicates that this rule applies to all users.
- Channel—This defines the security level of the input channel to which the rule applies: Select one of the following options:
  - Secure—Indicates that this rule applies only to secure channels (console, SCP, SSH and HTTPS), not including the SNMP and XML channels.
  - Insecure—Indicates that this rule applies only to insecure channels (Telnet, TFTP and HTTP), not including the SNMP and XML channels.
  - Secure XML SNMP—Indicates that this rule applies only to XML over HTTPS and SNMPv3 with privacy.

- Insecure XML SNMP—Indicates that this rule applies only to XML over HTTP or and SNMPv1/v2and SNMPv3 without privacy.

- Read Permission—The read permissions associated with the rule. These can be the following:
  - Exclude—Lowest read permission. Users are not permitted to get sensitive data in any form.
  - Plaintext Only—Higher read permission than above ones. Users are permitted to get sensitive data in plaintext only.
  - Encrypted Only—Middle read permission. Users are permitted to get sensitive data as encrypted only.
  - Both (Plaintext and Encrypted)—Highest read permission. Users have both encrypted and plaintext permissions and are permitted to get sensitive data as encrypted and in plaintext

- Default Read Mode—All default read modes are subjected to the read permission of the rule. The following options exist, but some might be rejected, depending on the rule's read permission.
  - Exclude—Do not allow reading the sensitive data.
  - Encrypted—Sensitive data is presented encrypted.
  - Plaintext—Sensitive data is presented as plaintext.

Step 3 Click **Apply**. The settings are saved to the Running Configuration file.

Step 4 The following actions can be performed on selected rules:

- Add, Edit or Delete rules or Restore To Default.
- Restore All Rules to Default—Restore a user-modified default rule to the default rule.

SSL Server

The Secure Socket Layer (SSL) feature is used to open an HTTPS session to the device. An HTTPS session may be opened with the default certificate that exists on the device. Some browsers generate warnings when using a default certificate, since this certificate is not signed by a Certification Authority (CA). It is best practice to have a certificate signed by a trusted CA. By default, the device contains certificates that can be modified. HTTPS is enabled by default.

SSL Server Authentication Settings

Secure Sockets Layer (SSL) authentication is a protocol for creating a secure connection for user-server interactions. A server and a user are involved in every web interaction. Users frequently enter sensitive, personal information on websites, putting persons and systems at risk. Better authentication strengthens security, especially for sites that store financial, medical, or personal data. Stable, verifiable, and secure user interactions are required. The way that a server verifies that the user is a real person is by collecting information. There are a number of ways this can be done.

Step 1 Click **Security** > **SSL Server** > **SSL Server Authentication Settings.**

Information appears for certificate 1 and 2 in the SSL Server Key Table. These fields are defined in the Edit page except for the following fields:

- Valid From—Specifies the date from which the certificate is valid.
- Valid To—Specifies the date up to which the certificate is valid.
- Certificate Source—Specifies whether the certificate was generated by the system (Auto Generated) or the user (User Defined).

Step 2 The device includes 2 certificates. Only one of them is the active certificate which can be used for the HTTPS session. To define which certificate is active, in the SSL Active Certificate Number, select an active certificate (**1** or **2**).

Step 3 Click **Apply**.

Step 4 In the HTTPS Session Logging section, check **Enable** to enable. By enabling the HTTPS session logging, this will allow a user to track the progress of HTTPS session setup and tear-down, via syslog messages generated by the device.

Step 5 Click **Apply**.

Generate Certificate Request

A new self-signed certificate maybe required to replace the certificate found on the device. To create a new certificate, complete the following steps:

Step 1 Click **Generate Certificate Request**.

Step 2 Next, enter the following fields:

- Certificate ID—Select the certificate ID.
- Regenerate RSA Key—Check the checkbox to regenerate a RSA key.
- Key Length—Select the key length from one of the 2 options (2048 bits or 3072 bits).
- Common Name—Enter a name for the certificate.
- Organization Unit—Enter the organization unit.
- Organization Name—Enter the organization name.
- Location—Enter the location or city name.
- State—Enter the state or province.
- Country—Enter the name of the country.
- Certificate Request—The Begin Certificate Request will be displayed.
- *Duration—Displays the number of days that the certificate is valid for. (Range 30-1095, Default 730.

Note The Duration field can only be seen when trying to edit an existing certificate.

Step 3 Click **Generate Certificate Request**. The new certificate is generated and replaces existing one.

Step 4 To import a certificate signed by a CA, select an active certificate and click **Import Certificate**.

Step 5 Enter the following fields:

- Certificate ID—Select a certificate.
- Certificate Source—Displays that the certificate is auto-generated.
- Certificate—Copy in the received certificate.
- Import RSA Key—Pair-Select to enable copying in the new RSA key-pair.
- Public Key—Copy in the RSA public key.
- Private Key (Encrypted)—Select and copy in the RSA private key in encrypted form.
-

Step 6 Click **Apply** to apply the changes to the Running Configuration.

Step 7 Click the **Details** button to display the SSL certificate details.

Step 8 Next, click **Display Sensitive Data as Encrypted** to display this key as encrypted. When this button is clicked, the private keys are written to the configuration file in encrypted form (when **Apply** is clicked). When the text is displayed in encrypted form, the button becomes Display Sensitive Data as Plaintext enabling you to view the text in plaintext again.

What to do next

Viewing the Certificate Chain

If the device certificate was signed by an intermediate CA authority and not a CA root authority – the user will need to import the intermediate certificate(s) used to sign the device certificate and each certificate in the chain up to the root certificate. Intermediate certificates can be imported using the CA Certificate Settings. To view this certificate chain select Certificate 1 or 2 from the SSL Server Key Table and click Certificate Chain. This will open the Certificate Chain modal which will display the device certificate and any intermediate certificate part of the device certificate chain.

SSH Server

The SSH Server feature enables a remote users to establish SSH sessions to the device. This is similar to establishing a telnet session, except the session is secured.

The device, as a SSH server, supports SSH User Authentication which authenticates a remote user either by password, or by public key. At the same time, the remote user as a SSH client can perform SSH Server Authentication to authenticate the device using the device public key (fingerprint).

SSH Server can operate in the following modes:

- By Internally-generated RSA/DSA Keys (Default Setting)—An RSA and a DSA key are generated. Users log on the SSH Server application and are automatically authenticated to open a session on the device when they supply the IP address of the device.
- Public Key Mode—Users are defined on the device. Their RSA/DSA keys are generated in an external SSH server application, such as PuTTY. The public keys are entered in the device. The users can then open an SSH session on the device through the external SSH server application.

SSH User Authentication

If you use the SSH User Authentication page to create an SSH username for a user who is already configured in the local user database. You can prevent additional authentication by configuring the Automatic Login feature, which works as follows:

- Enabled—If a user is defined in the local database, and this user passed SSH Authentication using a public-key, the authentication by the local database username and password is skipped.

Note The configured authentication method for this specific management method (console, Telnet, SSH and so on) must be Local (i.e. not RADIUS or TACACS+).

- Not Enabled—After successful authentication by SSH public key, even if the username is configured in the local user database, the user is authenticated again, as per the configured authentication methods.

To enable authentication and add a user.

Step 1 Click **Security** > **SSH Server** > **SSH User Authentication**.

Step 2 Select the following fields:

- SSH User Authentication by Password—Select **Enable** to enable and perform authentication of the SSH client user using the username/password configured in the local database.
- SSH Session Logging— Select **Enable** to enable SSH session logging. The SSH session logging allows a user to track the progress of an SSH session setup and tear-down, via syslog messages generated by the device.
- SSH User Authentication by Public Key—Select **Enable** to enable authentication of the SSH client user using the public key.
- Automatic Login—Select **Enable** to enable SSH User Authentication by Public Key feature.

Step 3 Click **Apply**. The settings are saved to the Running Configuration file.

The following fields are displayed for the configured users:

- SSH User Name—User name of user.
- Key Type—Whether this is an RSA or DSA key.
- Fingerprint—Fingerprint generated from the public keys.

Step 4 Click **Add or Edit** to add or edit a user and enter the fields:

- SSH User Name—Enter a user name.
- Key Type—Select either RSA or DSA.
- Public Key—Copy the public key generated by an external SSH client application (like PuTTY) into this text box.

Step 5 Click **Apply** to save the new user.

The following fields are displayed for all active users:

- IP Address—IP address of the active user.
- SSH User Name—User name of the active user.
- SSH Version—Version of SSH used by the active user.
- Cipher—Cipher of the active user.
- Authentication Code—Authentication code of the active user.

SSH Server Authentication

A remote SSH client can perform SSH Server Authentication to ensure it's establishing an SSH session to the expected SSH driver. To perform SSH Server Authentication, the remote SSH client must have a copy of the SSH server public key (or fingerprint) of the target SSH server.

The SSH Server Authentication page generates/imports the private/public key for the device as an SSH server. A user should copy the SSH server public key (or fingerprint) of this device to the application if it's to perform an SSH Server Authentication on its SSH sessions. Public and private RSA and DSA keys are automatically generated when the device is booted from the factory defaults. Each key is also automatically created when the appropriate user-configured key is deleted by the user.

To regenerate an RSA or DSA key or to copy in an RSA/DSA key generated on another device, complete the following steps:

Step 1 Click **Security** > **SSH Server** > **SSH Server Authentication**.

The following fields are displayed for each key in the Fingerprint section:

- Key Type—RSA or DSA.
- Key Source—Auto Generated or User Defined.
- Fingerprint—Fingerprint generated from the key.

Step 2 Select either an RSA or DSA key.

Step 3 You can perform any of the following actions:

- Generate—Generates a key of the selected type.
- Edit—Enables you to copy in a key from another device. Enter the following fields:
  - Key Type—As described above
  - Public Key—Enter the public key.
  - Private Key—Select either Plaintext or Encrypted and enter the private key.

    Plaintext—Enter the key as plaintext.
  - Delete—Enables you to delete a key.
  - Details—Enables you to view the generated key. The Details window also enables you to click **Display Sensitive Data as Plaintext**. If this is clicked, the keys are displayed as plaintext and not in encrypted form. If the key

is already being displayed as plaintext, you can click **Display Sensitive Data as Encrypted**. to display the text in encrypted form.

- Click **Apply** to save the settings.

SSH Client

A SSH client helps the user manage a network composed of one or more switches in which various system files are stored on a central SSH server. When configuration files are transferred over a network, the Secure Copy (SCP), which is an application that utilizes the SSH protocol, ensures that sensitive data, such as username/password cannot be intercepted.

The SSH client, only communicates with a trusted SSH server. When SSH server authentication is disabled (the default setting), any SSH server is considered trusted. When SSH server authentication is enabled, the user must add an entry for the trusted servers to the Trusted SSH Servers Table.

In general the SSH protocol can be used for two purposes, file transfers and terminal access.

SSH User Authentication

When a device (SSH client) attempts to establish a SSH session to a SSH server, the SSH server uses various methods for client authentication. Use this page to select an SSH user authentication method, set a username and password on the device, if the password method is selected or generate an RSA or DSA key, if the public/private key method is selected.

To select an authentication method, and set the username/password/keys, follow these steps:

Step 1 Click **Security** > **SSH Client** > **SSH User Authentication**.

Step 2 Under Global Configuration, select an SSH User Authentication Method. This is the global method defined for the secure copy (SCP). Select one of the options:

- By Password—This is the default setting. If this is selected, enter a password or retain the default one.
- By RSA Public Key—If this is selected, create an RSA public and Private key in the SSH User Key Table block.
- By DSA Public Key—If this is selected, create a DSA public/private key in the SSH User Key Table block.

Step 3 Under Credentials, enter the Username (no matter what method was selected) or user the default username. This must match the username defined on the SSH server.

Step 4 If the By Password method was selected, enter a password (Encrypted or Plaintext) or leave the default encrypted password.

Step 5 Perform one of the following actions:

- Apply—The selected authentication methods are associated with the access method.
- Restore Default Credentials—The default username and password (anonymous) are restored.
- Display Sensitive Data As Plaintext—Sensitive data for the current page appears as plaintext.

The SSH User Key Table contains the following fields for each key:

- Key Type—RSA or DSA.
- Key Source—Auto Generated or User Defined.
- Fingerprint—Fingerprint generated from the key.

Step 6 To handle an RSA or DSA key, select either RSA or DSA and perform one of the following actions:

- Generate—Generate a new key.
- Edit—Display the keys for copying/pasting to another device.
- Delete—Delete the key.
- Details—Display the Public and Private Key (Encrypted) for each SSH server type.

Note The public/private keys are encrypted and stored in the device memory. The keys are part of the device configuration file, and the private key can be displayed to the user, in encrypted or plaintext form.

SSH Server Authentication

To enable SSH server authentication and define the trusted servers, follow these steps:

Step 1 Click **Security** > **SSH Client** > **SSH Server Authentication**.

Step 2 Select **Enable** to enable SSH server authentication.

- IPv4 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address for messages used in communication with IPv4 SSH servers.
- IPv6 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address for messages used in communication with IPv6 SSH servers.

  Note If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 3 Click **Apply**.

Step 4 Click **Add** and enter the following fields for the Trusted SSH Server:

- Server Definition—Select one of the following ways to identify the SSH server:
  - By IP address—If this is selected enter the IP address of the server in the fields below.
  - By name—If this is selected enter the name of the server in the Server IP Address/Name field.
- IP Version—If you selected to specify the SSH server by IP address, select whether that IP address is an IPv4 or IPv6 address.
- IPv6 Address Type—If the SSH server IP address is an IPv6 address, select the IPv6 address type. The options are:
  - Link Local —The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link

local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

- Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

- Link Local Interface—Select the link local interface from the list of interfaces.
- Server IP Address/Name—Enter either the IP address of the SSH server or its name, depending on what was selected in Server Definition.
- Fingerprint—Enter the fingerprint of the SSH server (copied from that server).

Step 5 Click **Apply**. The trusted server definition is stored in the Running Configuration file.

Change User Password on SSH Server

Changing the password on the SSH Client Server only affects the remote SSH server. To change the password on the SSH server, follow these steps:

Step 1 Click **Security** > **SSH Client** > **Change User Password on SSH Server**.

Step 2 Enter the following fields:

- Server Definition—Define the SSH server by selecting either By IP Address or By Name. Enter the server name or IP address of the server in the Server IP Address/Name field.
- IP Version—If you selected to specify the SSH server by IP address, select whether that IP address is an IPv4 or IPv6 address.
- IPv6 Address Type—If the SSH server IP address is an IPv6 address, select the IPv6 address type. The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface from the list of interfaces.
- Server IP Address/Name—Enter either the IP address of the SSH server or its name, depending on what was selected in Server Definition.
- Username—This must match the username on the server.
- Old Password—This must match the password on the server.
- New Password—Enter the new password and confirm it in the Confirm Password field.

Step 3 Click **Apply**. The password on the SSH server is modified.

TCP/UDP Services

The TCP/UDP Services page enables TCP or UDP-based services on the device, usually for security reasons.

The device offers the following TCP/UDP services:

- HTTP-Enabled by factory default
- HTTPS-Enabled by factory default
- SNMP-Disabled by factory default
- Telnet-Disabled by factory default
- SSH-Disabled by factory default

To configure TCP/UDP services, follow these steps:

Step 1 Click **Security** > **TCP/UDP Services**.

Step 2 Enable or disable the following TCP/UDP services on the displayed services.

- HTTP Service-Indicates whether the HTTP service is enabled or disabled.
- HTTPS Service-Indicates whether the HTTPS service is enabled or disabled.
- SNMP Service-Indicates whether the SNMP service is enabled or disabled.
- Telnet Service-Indicates whether the Telnet service is enabled or disabled.
- SSH Service-Indicates whether the SSH server service is enabled or disabled.

Step 3 Click **Apply**. The services are written to the Running Configuration file.

The TCP Service Table displays the following fields for each service:

- Service Name-Access method through which the device is offering the TCP service.
- Type-IP protocol the service uses.
- Local IP Address-Local IP address through which the device is offering the service.
- Local Port-Local TCP port through which the device is offering the service.
- Remote IP Address-IP address of the remote device that is requesting the service.
- Remote Port-TCP port of the remote device that is requesting the service.
- State-Status of the service.

The UDP Service table displays the following information:

- Service Name-Access method through which the device is offering the UDP service.
- Type-IP protocol the service uses.
- Local IP Address-Local IP address through which the device is offering the service.
- Local Port-Local UDP port through which the device is offering the service.

- Application Instance-The service instance of the UDP service.

Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a traffic storm.

Storm protection enables you to limit the number of frames entering the device and to define the types of frames that are counted towards this limit.

When the rate of Broadcast, Multicast, or Unknown Unicast frames is higher than the user-defined threshold, frames received beyond the threshold are discarded.

Storm Control Settings

To define Storm Control, follow these steps:

Step 1 Click **Security** > **Storm Control** > **Storm Control Settings**.

Step 2 Select a port and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select the port for which storm control is enabled.

  Unknown Unicast Storm Control

- Storm Control State—Select to enable Storm Control for Unicast packets.
- Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Trap on Storm—Select to send a trap when a storm occurs on a port. If this isn't selected, the trap isn't sent.
- Shutdown on Storm—Select to shut down a port when a storm occurs on the port. If this isn't selected extra traffic is discarded.

  Multicast Storm Control

- Storm Control State—Select to enable Storm Control for Multicast packets.
- Multicast Type—Select one of the following types of Multicast packets on which to implement storm control:
  - All—Enables storm control on all Multicast packets on the port
  - Registered Multicast—Enables storm control only on registered Multicast addresses on the port
  - Unregistered Multicast—Enables only unregistered Multicast storm control on the port
- Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.

- Trap on Storm—Select to send a trap when a storm occurs on a port. If this isn't selected, the trap isn't sent.
- Shutdown on Storm—Select to shut down a port when a storm occurs on the port. If this isn't selected extra traffic is discarded.

  Broadcast Storm Control

- Storm Control State—Select to enable Storm Control for Broadcast packets.
- Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Trap on Storm—Select to send a trap when a storm occurs on a port. If this isn't selected, the trap isn't sent.
- Shutdown on Storm—Select to shut down a port when a storm occurs on the port. If this isn't selected extra traffic is discarded.

Step 4 Click **Apply**. Storm control is modified, and the Running Configuration file is updated.

Storm Control Statistics

To view Storm Control statistics, complete the following:

Step 1 Click **Security** > **Storm Control** > **Storm Control Statistics**.

Step 2 Select an interface.

Step 3 Select the Refresh Rate— The available options are:

No Refresh	Statistics aren't refreshed.
15 Sec	Statistics are refreshed every 15 seconds.
30 Sec	Statistics are refreshed every 30 seconds.
60 Sec	Statistics are refreshed every 60 seconds.

The following statistics are displayed for Unknown Unicast, Multicast and Broadcast Storm Control:

Multicast Traffic Type	(Only for Multicast Storm Control) All.
Bytes Passed	Number of bytes received.
Bytes Dropped	Number of bytes dropped because of storm control.
Last Drop Time	Time that the last byte was dropped.

Step 4 To clear all counters on all interfaces, click **Clear All Interfaces Counters**. To clear all counters on an interface, select it and click **Clear Interface Counters**.

Port Security

Note Port security cannot be enabled on ports on which 802.1X is enabled or on ports that defined as SPAN destination.

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured.

Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.

Port Security has four modes:

- Classic Lock—All learned MAC addresses on the port are locked, and the port doesn't learn any new MAC addresses. The learned addresses aren't subject to aging or relearning.
- Limited Dynamic Lock—The device learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the device doesn't learn additional addresses. In this mode, the addresses are subject to aging and relearning.
- Secure Permanent—Keeps the current dynamic MAC addresses associated with the port (as long as the configuration was saved to the Start configuration file). New MAC addresses can be learned as Permanent Secure ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.
- Secure Delete on Reset—Deletes the current dynamic MAC addresses associated with the port after reset. New MAC addresses can be learned as Delete-On-Reset ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.

When a frame from a new MAC address is detected on a port where it's not authorized (the port is classically locked, and there's a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- Frame is discarded.
- Frame is forwarded.
- Port is shut down.

When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address isn't learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.

To configure port security, complete the following:

Step 1 Click **Security** > **Port Security**.

Step 2 Select an interface to be modified, and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select the interface name.
- Interface Status—Select to lock the port.
- Learning Mode—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the Interface Status field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
  - Classic Lock—Locks the port immediately, regardless of the number of addresses that have already been learned.
  - Limited Dynamic Lock—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging of MAC addresses are enabled.
  - Secure Permanent—Keeps the current dynamic MAC addresses associated with the port and learns up to the maximum number of addresses allowed on the port (set by Max No. of Addresses Allowed). Relearning and aging are disabled.
  - Secure Delete on Reset—Deletes the current dynamic MAC addresses associated with the port after reset. New MAC addresses can be learned as Delete-On-Reset ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.
- Max No. of Addresses Allowed—Enter the maximum number of MAC addresses that can be learned on the port if Limited Dynamic Lock learning mode is selected. The number 0 indicates that only static addresses are supported on the interface.
- Action on Violation—Select an action to be applied to packets arriving on a locked port. The options are:
  - Discard—Discards packets from any unlearned source
  - Forward—Forwards packets from an unknown source without learning the MAC address
  - Shutdown—Discards packets from any unlearned source, and shuts down the port The port remains shut down until reactivated, or until the device is rebooted.
- Trap—Select to enable traps when a packet is received on a locked port. This is relevant for lock violations. For Classic Lock, this is any new address received. For Limited Dynamic Lock, this is any new address that exceeds the number of allowed addresses.
- Trap Frequency—Enter minimum time (in seconds) that elapses between traps.

Step 4 Click **Apply**. Port security is modified, and the Running Configuration file is updated.

802.1X Authentication

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicity-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles.

- Client or supplicant
- Authenticator

- Authentication server

A network device can be either a client/supplicant, authenticator or both per port.

Properties

The Properties page is used to globally enable port/device authentication. For authentication to function, it must be activated both globally and individually on each port.

To define port-based authentication, follow these steps:

Step 1 Click **Security > 802.1X Authentication > Properties**.

Step 2 Enter the parameters.

- Port-Based Authentication—Enable or disable port-based authentication.
- Authentication Method—Select the user authentication methods. The options are:
  - RADIUS, None—Perform port authentication first by using the RADIUS server. If no response is received from RADIUS, then no authentication is performed, and the session is permitted.
  - RADIUS—Authenticate the user on the RADIUS server. If no authentication is performed, the session isn't permitted.
  - None—Don't authenticate the user. Permit the session.
- Guest VLAN—Select to enable the use of a guest VLAN for unauthorized ports. If a guest VLAN is enabled, all unauthorized ports automatically join the VLAN selected in the Guest VLAN ID field. If a port is later authorized, it's removed from the guest VLAN. The guest VLAN can be defined as a layer 3 interface (assigned an IP address) like any other VLAN. However, device management isn't available via the guest VLAN IP address.
- Guest VLAN ID—Select the guest VLAN from the list of VLANs.
- Guest VLAN Timeout—Define a time period as either Immediate or enter a value in User Defined. This value is used as follows:

  After linkup, if the software doesn't detect the 802.1X supplicant, or the authentication has failed, the port is added to the guest VLAN, only after the Guest VLAN timeout period has expired.

  If the port state changes from Authorized to Not Authorized, the port is added to the guest VLAN only after the Guest VLAN timeout has expired.
- Trap Settings—To enable traps, select one of more of the following options:
  - 802.1x Authentication Failure Traps—Select to generate a trap if 802.1x authentication fails.
  - 802.1x Authentication Success Traps—Select to generate a trap if 802.1x authentication succeeds.

Step 3 Click **Apply**. The 802.1X properties are written to the Running Configuration file.

Port Authentication

The Port Authentication page enables configuration of parameters for each port. Since some of the configuration changes are only possible while the port is in Force Authorized state, such as host authentication, it's recommended that you change the port control to Force Authorized before making changes. When the configuration is complete, return the port control to its previous state.

Note A port with 802.1x defined on it can't become a member of a LAG. 802.1x and Port Security can't be enabled on same port at same time. If you enable port security on an interface, the Administrative Port Control can't be changed to Auto mode.

To define 802.1X authentication:

Step 1 Click **Security** > **802.1X Authentication** > **Port Authentication**.

Step 2 Select a port and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select a port.
- Current Port Control—Displays the current port authorization state. If the state is Authorized, the port is either authenticated or the Administrative Port Control is Force Authorized. Conversely, if the state is Unauthorized, then the port is either not authenticated or the Administrative Port Control is Force Unauthorized. If supplicant is enabled on an interface, the current port control is Supplicant.
- Administrative Port Control—Select the Administrative Port Authorization state. The options are:
  - Force Unauthorized—Denies the interface access by moving the interface into the unauthorized state. The device doesn't provide authentication services to the client through the interface.
  - Auto—Enables port-based authentication and authorization on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - Force Authorized—Authorizes the interface without authentication.
- Guest VLAN—Select to enable using a guest VLAN for unauthorized ports.
- Periodic Reauthentication—Select to enable port reauthentication attempts after the specified Reauthentication Period.
- Reauthentication Period—Enter the number of seconds after which the selected port is reauthenticated.
- Reauthenticate Now—Select to enable immediate port reauthentication.
- Authenticator State—Displays the defined port authorization state. The options are:
  - Initialize—In process of coming up.
  - Force-Authorized—Controlled port state is set to Force-Authorized (forward traffic).
  - Force-Unauthorized—Controlled port state is set to Force-Unauthorized (discard traffic).

Note If the port isn't in Force-Authorized or Force-Unauthorized, it's in Auto Mode and the authenticator displays the state of the authentication in progress. After the port is authenticated, the state is shown as Authenticated.

- Time Range—Select to enable limiting authentication to a specific time range.
- Time Range Name—If Time Range is selected, click the Edit button to be redirected to the time range page and select the time range name to be used.
- Max Hosts—Enter the maximum number of authorized hosts allowed on the interface.

  Select either Infinite for no limit, or User Defined to set a limit.

  Note Set this value to 1 to simulate single-host mode for web-based authentication in multi-sessions mode.

- Quiet Period—Enter the length of the quiet period.
- Resending EAP—Enter the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
- Max EAP Requests—Enter the maximum number of EAP requests that will be sent. If a response isn't received after the defined period (supplicant timeout), the authentication process is restarted.
- Supplicant Timeout—Enter the number of seconds that lapses before EAP requests are resent to the supplicant.
- Server Timeout—Enter the number of seconds that lapses before the device resends a request to the authentication server.

Step 4 Click **Apply**. The port settings are written to the Running Configuration file.

Host and Session Authentication

The Host and Session Authentication page enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

To define 802.1X advanced settings for ports, complete the following steps:

Step 1 Click **Security** > **802.1X Authentication** > **Host and Session Authentication**.

Step 2 Select a port, and click **Edit.**

Step 3 Enter the parameters.

- Interface—Enter a port number for which host authentication is enabled.
- Host Authentication—Select from one of the following modes.
  - Single Host—A port is authorized if there is an authorized client. Only one host can be authorized on a port.
  - Multiple Host (802.1X)—A port is authorized if there is if there is at least one authorized client.
  - Multiple Sessions—Unlike the single-host and multi-host modes, a port in the multi-session mode does not have an authentication status. This status is assigned to each client connected to the port.

Single Host Violation Settings—Can only be chosen if host authentication is Single Host.

- Action on Violation—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address isn't the supplicant MAC address. The options are:
  - Protect (Discard)—Discards the packets.
  - Restrict (Forward)—Forwards the packets.
  - Shutdown—Discards the packets and shuts down the port. The ports remain shut down until reactivated, or until the device is rebooted.
- Traps—Select to enable traps.
- Trap Frequency—Defines how often traps are sent to the host. This field can be defined only if multiple hosts are disabled.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

The Host and Session Authentication Table will display the number of violations under the Number of Violations column.

Authenticated Hosts

To view details about authenticated users, click. **Security** > **802.1X Authentication** > **Authenticated Hosts**.

This page displays the following fields:

- User Name—Supplicant names that authenticated on each port.
- Port—Number of the port
- Session Time (DD:HH:MM:SS)—Amount of time that the supplicant was authenticated and authorized access at the port.
- Authentication Server—RADIUS server
- MAC Address—Displays the supplicant MAC address.

Denial of Service Prevention

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users.

DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

One method of resisting DoS attacks employed by the device is the use of Secure Core Technology (SCT), which is enabled by default and cannot be disabled. The Cisco device is an advanced device that handles management traffic, protocol traffic and snooping traffic, in addition to end-user (TCP) traffic. SCT ensures that the device receives and processes management and protocol traffic, no matter how much total traffic is received. This is done by rate-limiting TCP traffic to the CPU.

Security Suite Settings

Note Before activating DoS Prevention, you must unbind all Access Control Lists (ACLs) or advanced QoS policies that are bound to a port. ACL and advanced QoS policies aren't active when a port has DoS Protection enabled on it.

To configure DoS Prevention global settings and monitor SCT:

Step 1 Click **Security** > **Denial of Service Prevention** > **Security Suite Settings**.

CPU Protection Mechanism: Enabled indicates that SCT is enabled.

Step 2 Click **Details** beside CPU Utilization to go to the CPU Utilization page and view CPU resource utilization information.

Step 3 Click **Edit** beside TCP SYN Protection to set the feature.

Step 4 Configure the DoS Prevention settings:

- Disable-Disable all types of Denial of Service features (except device level TCP SYN protection).
- System-Level Prevention-Enable preventing attacks from Stacheldraht Distribution, Invasor Trojan, Back Orifice Trojan and Martian Addresses.
- System-Level and Interface-Level Prevention-In addition to the system-level prevention, you can enable and configure the following interface-level settings: Syn Filtering, Syn Rate Protection, ICMP Filtering and IP Fragmented.

Step 5 If System-Level Prevention or System-Level and Interface-Level Prevention is selected, enable one or more of the following Denial of Service Protection options:

- Stacheldraht Distribution-Discards TCP packets with source TCP port equal to 16660.
- Invasor Trojan-Discards TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
- Back Orifice Trojan-Discards UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

Step 6 Click the following as required:

- Martian Addresses-Click **Edit** to go to the Martian Addresses, on page 34 page.
- SYN Filtering-Click **Edit** to go to the SYN Filtering, on page 35 page.
- SYN Rate Protection-(In Layer 2 only) Click **Edit** to go to the SYN Rate Protection, on page 35 page.
- ICMP Filtering-Click **Edit** to go to the ICMP Filtering, on page 36 page.
- IP Fragmented-Click **Edit** to go to the IP Fragments Filtering, on page 36 page.

Step 7 Click **Apply**. The Denial of Service prevention Security Suite settings are written to the Running Configuration file.

SYN Protection

The network ports might be used by hackers to attack the device in a SYN attack, which consumes TCP resources (buffers) and CPU power.

Since the CPU is protected using SCT, TCP traffic to the CPU is limited. However, if one or more ports are attacked with a high rate of SYN packets, the CPU receives only the attacker packets, thus creating Denial-of-Service.

When using the SYN protection feature, the CPU counts the SYN packets ingressing from each network port to the CPU per second.

To configure SYN protection, follow these steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Protection**.

Step 2 Enter the parameters.

- Block SYN-FIN Packets-Select to enable the feature. All TCP packets with both SYN and FIN flags are dropped on all ports.
- SYN Protection Mode-Select between three modes:
  - Disable-The feature is disabled on a specific interface.
  - Report-Generates a SYSLOG message. The status of the port is changed to Attacked when the threshold is passed
  - Block and Report-When a TCP SYN attack is identified, TCP SYN packets destined for the system are dropped and the status of the port is changed to Blocked.
- SYN Protection Threshold-Number of SYN packets per second before SYN packets will be blocked (deny SYN with MAC-to-me rule will be applied on the port).
- SYN Protection Period-Time in seconds before unblocking the SYN packets (the deny SYN with MAC-to-me rule is unbound from the port).

Step 3 Click **Apply**. SYN protection is defined, and the Running Configuration file is updated.

The SYN Protection Interface Table displays the following fields for every port or LAG (as requested by the user).

- Current Status-Interface status. The possible values are:
  - Normal-No attack was identified on this interface.
  - Blocked-Traffic isn’t forwarded on this interface.
  - Attacked-Attack was identified on this interface.
- Last Attack-Date of last SYN-FIN attack identified by the system and the system action.

Martian Addresses

The Martian Addresses page enables entering IP addresses that indicate an attack if they are seen on the network. Packets from these addresses are discarded. The device supports a set of reserved Martian addresses that are illegal from the point of view of the IP protocol. The supported reserved Martian addresses are:

- Addresses defined to be illegal in the Martian Addresses page
- Addresses that are illegal from the point of view of the protocol, such as loopback addresses, including addresses within the following ranges:
  - 0.0.0.0/8 (Except 0.0.0.0/32 as a Source Address)-Addresses in this block refer to source hosts on this network.
  - 127.0.0.0/8-Used as the Internet host loopback address
  - 192.0.2.0/24-Used as the TEST-NET in documentation and example codes
  - 224.0.0.0/4 (As a Source IP Address)-Used in IPv4 Multicast address assignments, and was formerly known as Class D Address Space.
  - 240.0.0.0/4 (Except 255.255.255.255/32 as a Destination Address)-Reserved address range, and was formerly known as Class E Address Space.

You can also add new Martian Addresses for DoS prevention. Packets that have a Martian address are discarded.

To define Martian addresses, follow these steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **Martian Addresses**.

Step 2 Select **Reserved Martian Addresses** and click **Apply** to include the reserved Martian Addresses in the System Level Prevention list.

Step 3 To add a Martian address click **Add**.

Step 4 Enter the parameters.

- IP Version-Indicates the supported IP version. Currently, support is only offered for IPv4.
- IP Address-Enter an IP address to reject. The possible values are:
  - From Reserved List-Select a well-known IP address from the reserved list.
  - New IP Address-Enter an IP address.
- Mask-Enter the mask of the IP address to define a range of IP addresses to reject. The values are:
  - Network Mask-Network mask in dotted decimal format
  - Prefix Length-Enter the prefix of the IP address to define the range of IP addresses for which Denial of Service prevention is enabled.

Step 5 Click **Apply**.

SYN Filtering

The SYN Filtering page enables filtering TCP packets that contain a SYN flag, and are destined for one or more ports.

To define a SYN filter, complete the following steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Filtering**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the filter is defined.
- IPv4 Address—Enter the IP address for which the filter is defined, or select All addresses.
- Network Mask—Enter the network mask for which the filter is enabled in IP address format. Enter one of the following:
  - Mask—Network mask in dotted decimal format
  - Prefix length—Enter the Prefix length of the IP address to define the range of IP addresses for which Denial of Service prevention is enabled.
- TCP Port—Select the destination TCP port being filtered:
  - Known ports—Select a port from the list.
  - User Defined—Enter a port number.
  - All ports—Select to indicate that all ports are filtered.

Step 4 Click **Apply**. The SYN filter is defined, and the Running Configuration file is updated.

SYN Rate Protection

The SYN Rate Protection page enables limiting the number of SYN packets received on the ingress port. This can mitigate the effect of a SYN flood against servers, by rate limiting the number of new connections opened to handle packets.

To define SYN rate protection, complete the following steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Rate Protection**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the rate protection is being defined.
- IP Address—Enter the IP address for which the SYN rate protection is user defined or select All addresses. If you enter the IP address, enter either the mask or prefix length.

- Network Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix length—Select the Prefix length and enter the number of bits that comprise the source IP address prefix.
- SYN Rate Limit—Enter the number of SYN packets that be received.

Step 4 Click **Apply**. The SYN rate protection is defined, and the Running Configuration is updated.

ICMP Filtering

The ICMP Filtering page enables the blocking of ICMP packets from certain sources. This can reduce the load on the network in case of an ICMP attack.

To configure the ICMP filtering, complete the following steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **ICMP Filtering**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the ICMP filtering is being defined.
- IP Address—Enter the IPv4 address for which the ICMP packet filtering is activated or select All addresses to block ICMP packets from all source addresses. If you enter the IP address, enter either the mask or prefix length.
- Network Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
  - Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix length—Select the Prefix length and enter the number of bits that comprise the source IP address prefix.

Step 4 Click **Apply**. The ICMP filtering is defined, and the Running Configuration is updated.

IP Fragments Filtering

IP fragmentation occurs when the data of the network layer is too large to be transmitted over the data link layer in one piece. Then the data of the network layer is split into several pieces (fragments), and this process is called IP fragmentation.

To configure fragmented IP filtering and block fragmented IP packets, complete the following steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **IP Fragments Filtering**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the IP fragmentation is being defined.
- IP Address—Enter an IP network from which the fragmented IP packets is filtered or select All addresses to block IP fragmented packets from all addresses. If you enter the IP address, enter either the mask or prefix length.
- Network Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix length—Select the Prefix length and enter the number of bits that comprise the source IP address prefix.

Step 4 Click **Apply**. The IP fragmentation is defined, and the Running Configuration file is updated.

Certificate Settings

The Cisco Business Dashboard Probe (CBD) and Plug-n-Play (PNP) features require CA certificates to establish HTTPS communication with the CBD or PNP servers. The Certificate Settings feature allows these applications and device managers to do the following:

- Install trusted CA certificates and to remove certificates that are no longer wanted
- Statically add certificates to device configuration file
- Manage a revocation list of untrusted certificates

In addition, the Certificate Settings feature can be used to import intermediate certificates that create the device HTTPS server certificate chain. For more details, please see SSL Server Authentication Settings , on page 15.

Note The validity of the certificates is based on the system clock. Use the default system clock or it does not provide proper validation. Therefore, make sure the system clock is based on device Real time clock (if supported) or was actively set since the last reboot (preferably via SNTP service). If the system clock is not based on RTC or was not set since last reboot validation of certificate will fail, even if the system clock is within the validity date of the certificate.

Dynamic Certificates

The CBD and PNP applications can install dynamic trusted certificates to the device memory. The installed certificate must include the following attributes:

- Certificate name — A string that is used to identify the certificate.
- Owner— The application name that installed the certificate (for example, PNP, CBD)
- The certificate itself in PEM format.

An application can also delete a specific or all dynamic certificates installed by that application.

Considerations

- Up to 512 dynamic certificates can be installed on the device.
- Dynamic certificates are removed when the device reboots

Static Certificates

If an application wants to add a certificate that will not be deleted on reset, or if a user of the switch wants to add a certificate, they can add a static certificate including an intermediate certificate(s) used to sign the device HTTPS server certificate. These certificates are saved in the device running configuration and can be copied to the startup configuration.

Adding a static certificate requires providing the following attributes:

- Certificate name —This is a string that is used to identify the certificate.
- Owner— the name of the application that installed the certificate (for example, PNP, CBD), or "static" if certificate is added by a user.
- The certificate itself in PEM format.

Considerations

- Up to 256 static certificates can be installed on the device.
- It is possible for identical certificates to be added by different applications or users as long as the names used to identify them are different.

CA Certificate Setting

Users can access information on all installed certificates (dynamic and static). The following information is displayed per each certificate:

Step 1 Click **Security** > **Certificate Settings** > **CA Certificate Settings**.

Step 2 To import a new certificate, click **Add** and complete the following:

- Certificate Name—Enter the name of the certificate.
- Certificate Type — Select the type of certificate- root (the default) or intermediate (part of device HTTPs server certificate chain).
- Certificate—Paste the certificate in PEM format (including the begin and end marker lines).

Step 3 Click **Apply** to apply the new settings.

Step 4 To view the details of an existing certificate, select the certificate from the list and click **Details**. The following will be displayed:

Option	Description
Certificate Name	The name or unique identifier of the certificate.
Type	This can be signer, static or dynamic.

Option	Description
CA Type	Can be either Root or Intermediate or N/A (for the signer certificate).
Owner	This can be signer, static, CBD or PNP
Version	The version of the certificate.
Serial Number	The serial number of the certificate.
Status	The status of the certificate.
Valid From	The date and time from which certificate is valid,
Valid To	The date and time until which the certificate is valid.
Issuer	The entity or CA that signed the certificate.
Subject	Distinguished name (DN) information for the certificate.
Public Key Type	The type of the public key.
Public Key Length	The length (in bits) of the public key.
Signature Algorithm	The cryptographic algorithm used by the CA to sign the certificate.
Certificate	The certificate details in PEM format.

Step 5 You can use the following filters to find a specific certificate.

- Type equals to—Check this box and select Signer, Static, or Dynamic from the drop-down list, to filter by these certificate types.
- Owner equals to—Paste the certificate in PEM format (including the begin and end marker lines).

Step 6 To remove one or more certificates select the certificate(s) and press **Delete**. Only Static certificates can be deleted.

CA Certificate Revocation List

If a certificate becomes untrusted for any reason, it can be added to the revocation list by the user or one of the applications. If a certificate is included in the revocation list, it is considered non-valid and the device will not allow it to be used. Adding a certificate to the revocation list will not remove the revoked certificate from the certificate database. It will only update its status to Not Valid (Revoked). When a certificate is removed from the revocation list, its status is automatically updated in the certificate database. There is no need to re-install it.

To add or remove a certificate to/from the revocation list, complete the following:

Step 1 Click **Security** > **Certificate Settings** > **CA Certificate Revocation List**.

Step 2 Click **Add** to open the Add Revoked Certificate dialog box

Step 3 Provide the following details:

- Issuer—The string identifying the issuer (for example: "C=US, O=MyTrustOrg, CN=MyCommonName") (0-160 chars).
- Serial Number—The serial number of the revoked certificate. This is a string of hexadecimal pairs (length 2-40).

Step 4 Click **Apply** to add the certificate.

Considerations

- Up to 512 certificates can be added to the revocation list.
- All certificates that match the entry in the revocation list are considered not valid (even if they are identified under different names in the certificate database).

Step 5 To delete an existing certificate, select the certificate from the Revoked CA Certificate Table and click **Delete**.