System Profile

AAA

The authentication, authorization, and accounting (AAA) feature helps authenticate users logging in to the Cisco SD-Routing device, decide what permissions to give them, and perform accounting of their actions.

The following tables describe the options for configuring the AAA feature.

Local

Field	Description
Add AAA User	
Name	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved.
Password	Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, The YANG 1.1 Data Modeling Language. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommended that you change this password.

Field	Description
Confirm Password	Re-enter the password for the user.
Privilege	Select between privilege level 1 or 15. • Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command. • Level 15: Privileged EXEC mode. Full access to all commands, such as the reload command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
Add Public Key Chain	
SSH RSA Key	Choose **ssh-rsa**.

Radius

Field	Description
Add Radius Server	
IP Address (v4 or v6)	Enter the IP address of the RADIUS server host.
Acct Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 through 65535. Default: 1813
Auth Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Default: 1812
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 seconds
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key*	Enter the key the Cisco SD-Routing device passes to the RADIUS server for authentication and encryption.
Key Type	Choose Protected Access Credential (PAC) or key type.

TACACS Server

Field	Description
Add TACACS Server	
IP Address (v4 or v6)	Enter the IP address of the TACACS+ server host.
Authentication Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. Default: 49
Timeout [second]	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key	Enter the key the Cisco SD-Routing device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

Accounting

Field	Description
Add Accounting Rule	
Rule Id	Enter the accounting rule ID.
Method	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
Start Stop	Enable this option to if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Groups	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

Authorization

Field	Description
Console	Enable this option to perform authorization for console access commands.
Config Commands	Enable this option to perform authorization for configuration commands.
Add Authorization Rule	
Rule Id	Enter the authorization rule ID.
Method	Choose **Commands**, which causes commands that a user enters to be authorized.
Level	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.
Authenticated	Enable this option to apply the authorization rule parameters only to the authenticated users. If you do not enable this option, the rule is applied to all users.
Group(s)	Choose a previously configured TACACS group. The parameters that this authorization rule defines are used by the TACACS servers that are associated with this group.

802.1x

Field	Description
Authentication Param	Enable authentication parameters.
Accounting Param	Enable accounting parameters

Authentication and Authorization Order

Field	Description
Server Auth Order	Select **local**.

Banner

The Banner feature helps you to configure the system login banner.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and choose one of the following:

The following table describes the options for configuring the Banner feature.

Field	Description
Name	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Login	Enter the text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type \n.
Message of the Day	Enter the message-of-the-day text to display before the login banner. The string can be up to 2048 characters long. To insert a line break, type \n.

Global

The Global feature helps you enable or disable various services on the devices such as HTTP, HTTPS, Telnet, IP domain lookup, and several other device settings.

The following tables describe the options for configuring the Global feature.

Services

Field	Description
HTTP Server	Enable or disable HTTP server.
HTTPS Server	Enable or disable secure HTTPS server.
FTP Passive	Enable or disable passive FTP.
Domain Lookup	Enable or disable Domain Name System (DNS) lookup.
ARP Proxy	Enable or disable proxy ARP.
RSH/RCP	Enable or disable remote shell (RSH) and remote copy (rcp) on the device.
Line Virtual Teletype (Configure Outbound Telnet)	Enable or disable outbound telnet.
Cisco Discovery Protocol (CDP)	Enable or disable Cisco Discovery Protocol (CDP).
Link Layer Discovery Protocol (LLDP)	Enable or disable Link Layer Discovery Protocol (LLDP).
HTTP Client Source Interface	Enter the address of the source interface in all HTTPS client connections.

NAT

Field	Description
NAT 64 UDP Timeout	Specify the NAT64 translation timeout for UDP. Range: 1 to 536870 (seconds) Default: 300 seconds (5 minutes)
NAT 64 TCP Timeout	Specify the NAT64 translation timeout for TCP. Range: 1 to 536870 (seconds) Default: 3600 seconds (1 hour)
NAT TCP Timeout	Specify when NAT translations over TCP sessions time out Range: 1 through 8947 minutes Default: 3600 seconds (1 hour)
NAT 64 UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 300 seconds (5 minutes)

Authentication

Field	Description
HTTP Authentication	Choose the HTTP authentication mode. Accepted values: Local, AAA Default: Local

SSH Version

Field	Description
SSH Version	Choose the SSH version. Default: Disabled

Other Settings

Field	Description
TCP Keepalives (In)	Enable or disable generation of keepalive timers when incoming network connections are idle.
TCP Keepalives (Out)	Enable or disable generation of keepalive timers when outgoing network connections are idle.

Field	Description
TCP Small Servers	Enable or disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable or disable small UDP servers (for example, ECHO).
Console Logging	Enable or disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination.
VTY Line Logging	Enable or disable the device to display log messages to a vty session in real time.
SNMP IFINDEX Persist	Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable or disable BOOTP server. When enabled, the device listens for the BOOTP packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.

Logging

The Logging feature helps you configure logging to either the local hard drive or a remote host.

The following tables describe the options for configuring the Logging feature.

Field	Description
Max File Size(In Megabytes)	Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds the configured value, the file is rotated and the syslog process is notified. Range: 1 to 20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files. Range: 1 to 10 Default: 10

TLS Profile

Field	Description
Add TLS Profile	
TLS Profile Name	Enter the name of the TLS profile.

Field	Description
TLS Version	Choose a TLS version: • **TLSv1.1** • **TLSv1.2**
Authentication Type*	Choose **Server**.
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. The following is the list of cipher suites. • **aes-128-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_128_sha • **aes-256-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_256_sha • **dhe-aes-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above) • **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB • **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above) • **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above) • **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **rsa-aes-gcm-sha2**: Encryption type tls_rsa_with_aes_gcm_sha2 (TLS1.2 and above)

Server

Field	Description
Add Server	
IPv4 Address	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VRF	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 0 through 65530

Field	Description
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.
Severity	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of the following: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable	Enable this option to allow syslog over TLS. When you enable this option, the following field appears: **TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears: **TLS Properties Profile**: Choose a TLS profile that you have created for server or mutual authentication in the IPv4 server configuration.
Add IPv6 Server	
IPv6 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VRF	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 0 through 65530
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Field	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of the following: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable	Enable this option to allow syslog over TLS.
TLS Properties Custom Profile*	Enable this option to choose a TLS profile.
TLS Properties Profile	Choose a TLS profile that you have created for server or mutual authentication in the IPv6 server configuration.

NTP

Network Time Protocol (NTP) is a protocol that allows a distributed network of servers and clients to synchronize the timekeeping across the network. The NTP feature helps you configure NTP settings on the Cisco SD-WAN network.

The following tables describe the options for configuring the NTP feature.

Server

Field	Description
Add Server	
Hostname/IP address	Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server.
VRF to reach NTP Server*	Enter the VRF name used to reach the NTP server, can be up to 32 alphanumeric characters

Field	Description
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the **Trusted Key** field under **Authentication**.
Set NTP version	Enter the version number of the NTP protocol software. Range: 1 to 4 Default: 4
Set interface to use to reach NTP server	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer this NTP server*	Enable this option if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, Cisco SD-Routing chooses the one at the highest stratum level.

Authentication

Field	Description
Add Authentication Keys	
Key Id	Enter an MD5 authentication key ID. Range: 1 to 65535
MD5 Value*	Enter an MD5 authentication key. Enter either a cleartext key or an AES-encrypted key.

Advanced

Field	Description
Authoritative NTP Server	Choose **Global** from the drop-down list, and enable this option if you want to configure one or more supported routers as a primary NTP router. When you enable this option, the following field appears: **Stratum**: Enter the stratum value for the primary NTP router. The stratum value defines the hierarchical distance of the router from its reference clock. Valid values: Integers 1 to 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 8.
Source	Enter the name of the exit interface for NTP communication. If configured, the system sends NTP traffic to this interface. For example, enter **`GigabitEthernet1`** or **`Loopback0`**.

SNMP

The application-layer Simple Network Management Protocol (SNMP) provides a communication standard for interaction between SNMP managers and agents. The protocol defines a standardized language that is commonly used for monitoring and managing devices in a network. The SNMP feature helps you configure the SNMP functionality on the Cisco SD-Routing devices.

The following tables describe the options for configuring the SNMP feature.

SNMP

Table 1: Advanced

Field	Description
Shutdown	By default, SNMP is enabled.
Contact Person	Enter the name of the network management contact person in charge of managing the Cisco SD-Routing device. It can be a maximum of 255 characters.
Location of Device	Enter a description of the location of the device. It can be a maximum of 255 characters.

SNMP Version

Table 2: Basic

Field	Description
SNMP Version	Choose one of the following SNMP versions: • **SNMP v2** • **SNMP v3**
SNMP v2: Add View	
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 255 characters. You must add a view name for all views before adding a community.
Add OID	Click this option to add object identifiers (OID) and configure the following parameters: • **Id**: Enter the OID of the object. For example, to view the internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Cisco SD-Routing device MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • **Exclude**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view.

Flexible Port Speed

The Flexible Port Speed feature is applicable only to the Cisco Catalyst 8500-12X4QC router. Use this feature to configure interfaces to work as 100GE, 40GE, 10GE, or 1GE based on your requirement. Any changes made to the port type take effect only after applying the configuration group to devices.

Updating the port configuration using the Flexible Port Speed feature may enable some ports and disable others. For instance, by default , C8500-12X4QC operates Bay 1 in 10GE mode and Bay 2 in 40GE mode. The Bay 1 mode can be 10GE, 40GE, or 100GE. Setting Bay 1 to 100GE disables all ports of Bay 0. For more information, see Bay Configuration of the Cisco Catalyst 8500-12X4QC device.

For more information about the Cisco Catalyst 8500-12X4QC platform's port options in each of its bays, see the C8500-12X4QC product overview in the *Cisco Catalyst 8500 Series Edge Platforms Data Sheet*.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.
Device Specific (Indicated by a host icon)	Use a device-specific value for the parameter. Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the field. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Default (indicated by a check mark)	The default value appears for parameters that have a default setting.

Basic Settings

Parameter Name	Description
Port Type	Choose from one of the following port combinations: • **12 ports of 1/10GE + 3 ports of 40GE** • **8 ports of 1/10GE + 4 ports of 40GE** • **2 ports of 100GE** • **12 ports of 1/10GE + 1 port of 100GE** • **8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE** • **3 ports of 40GE + 1 port of 100GE** Default is 12 ports of 1/10GE + 3 ports of 40GE.