Cisco Expressway REST API

Reference Guide

First Published: June 2016

Last Updated: July 2017

X8.10

Contents

Preface

Change History

Table 1 Reference Guide Change History

Date	Change	Reason
July 2017	Phase three of REST API. Now includes firewall rules, SIP, and domain certificates.	Released with X8.10
January 2017	Updated with HTTP allow list calls and get by filter option.	Released with X8.9.1
December 2016	Phase two of REST API. Now includes B2B functionality and ability to delete.	Released with X8.9
June 2016	First phase of REST API to set up Mobile and Remote Access (MRA).	Released with X8.8

Introduction

Welcome to the Expressway REST API documentation. The Expressway REST API is compliant with RAML version 0.8 (raml.org/spec.html). Although the API is fully compliant, it does not support nested APIs.

Schemas

All request and response schema on the Expressway REST API use JSON Schema version 4 (json-schema.org/documentation.html) . Request parameters are not supported and only JSON schemas are used.

Authentication

The API is only accessible via HTTPS and requires authentication. The authentication credentials are the administrator credentials on the Expressway node.

Base URI

The base URI to access the Expressway REST API is as follows: http://<external_address>/api/provisioning (for example, `http://10.0.0.1/api/provisioning`).

The REST API is published in the following categories:

- Cisco Expressway-E:
  `/edge/ <remaining path>` (for example , `http://10.0.0.1/api/provisioning/edge/credential`).
- Cisco Expressway-C:
  `/controller/ <remaining path>` (for example, `http://10.0.0.1/api/provisioning/controller/domain`).
- Common between Cisco Expressway-E and Cisco Expressway-C:
  `/common/<remaining path>` (for example, `http://10.0.0.1/api/provisioning/common/certs/root`).
- You can also filter your Get requests in order to find a specific entry. For example, `/controller/zone/traversalclient/name/myzone` would return the traversal client zone called `myzone`.

Authentication

/certs/generate_csr:

Generate, read or delete the Certificate Signing Request (CSR).

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Additional_FQDNS:** Additional free-form hostnames included in the certificate. **Country:** The two-letter ISO code for the country where your organization is located. **KeyLength:** The number of bits used for public and private key encryption. Default: 4096. **DigestAlgorithm:** The Digest algorithm used for the signature. Default: SHA-256. **Province:** The province, region, county, or state where your organization is located. **Locality:** The town or city where your organization is located. **Organization:** The name of the organization or business. **OrganizationalUnit:** The department name or organizational unit handling the certificate. **Email:** The email address to include in the certificate. } ***Required:*** *Country, Province, Locality, Organization, OrganizationalUnit*.	Gets the generated CSR from its path and displays it.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **Additional_FQDNS:** Additional free-form hostnames included in the certificate. **Country:** The two-letter ISO code for the country where your organization is located. **KeyLength:** The number of bits used for public and private key encryption. Default: 4096. **DigestAlgorithm:** The Digest algorithm used for the signature. Default: SHA-256. **Province:** The province, region, county, or state where your organization is located. **Locality:** The town or city where your organization is located. **Organization:** The name of the organization or business. **OrganizationalUnit:** The department name or organizational unit handling the certificate. **Email:** The email address to include in the certificate. } ***Required:*** *Country, Province, Locality, Organization, OrganizationalUnit*.	200	{ **Message:** Success/Failure/Info message for the operation. }	Generates the CSR and stores it in its path.

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/Failure/Info message for the operation. }	Discard the generated CSR.

/certs/root:

Generate, read or delete the root certificate resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	Certificate content.	Get the root certificate from the default path.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **file:** File to upload. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Write the root certificate to the default path. The request body contains the root CA data.

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/Failure/Info message for the operation. }	Reset the root CA to its default state.

/certs/server:

Generate, read or delete the signed server certificate resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	Certificate content.	Get the server certificate from the default path.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **file:** File to upload. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Write the server certificate to the default path. The request body contains the server certificate data.

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/Failure/Info message for the operation. }	Reset the server certificate to its default state.

Common Between Cisco Expressway-C and Cisco Expressway-E

/common/adminaccount/configuration:

PUSH, GET or PUT onto local database for authentication.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AccessLevel:** The access level of the administrator account. Default: Read-Write. **ApiAccess:** Determines whether this account is allowed to access the systems status and configuration using the Application Programming Interface. Default: Yes. **EmergencyAccount:** Select Yes to make this the emergency account. This special local account can log in to the VCS even when the Administrator authentication source is set to Remote only. Default: No. **Name:** Enter the username of this administrator account. Administrator accounts enable people or external systems to access this system. This field is case sensitive. Range 1 to 128 characters. **State:** Disable the account if required. When you disable an account, all access is denied to that account. Default: Enabled. **WebAccess:** Determines whether this account is allowed to log in to the system using the web interface. Default: Yes. }	Fetch the admin account details.

Method	Request Body	Response Code	Response Body	Comment

POST	{ **AccessLevel:** The access level of the administrator account. Default: Read-Write. **ApiAccess:** Determines whether this account is allowed to access the systems status and configuration using the Application Programming Interface. Default: Yes. **ConfirmPassword:** Enter the password of this administrator account. Range: 1 to 1024. **EmergencyAccount:** Select Yes to make this the emergency account. This special local account can log in to the Expressway even when the Administrator authentication source is set to Remote only. Default: No. **Name:** Enter the username of this administrator account. Administrator accounts enable people or external systems to access this system. This field is case sensitive. Range 1 to 128 characters. **Password:** Enter the password of this administrator account. Range: 1 to 1024. **State:** Disable the account if required. When you disable an account, all access is denied to that account. Default: Enabled. **WebAccess:** Determines whether this account is allowed to log in to the system using the web interface. Default: Yes. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Create an admin account configuration.

Method	Request Body	Response Code	Response Body	Comment

PUT	{ **AccessLevel:** The access level of the administrator account. Default: Read-Write. **ApiAccess:** Determines whether this account is allowed to access the systems status and configuration using the Application Programming Interface. Default: Yes. **EmergencyAccount:** Select Yes to make this the emergency account. This special local account can log in to the Expressway even when the Administrator authentication source is set to Remote only. Default: No. **Name:** Enter the username of this administrator account. Administrator accounts enable people or external systems to access this system. This field is case sensitive. Range 1 to 128 characters. **NewName:** Enter the new username of this administrator account. Administrator accounts enable people or external systems to access this system. This field is case sensitive. Range: 0 to 128. **State:** Disable the account if required. When you disable an account, all access is denied to that account. Default: Enabled. **WebAccess:** Determines whether this account is allowed to log in to the system using the web interface. Default: Yes. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Update an admin account.

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/Failure/Info message for the operation. }	Reset the root CA to its default state.

common/adminaccount/changepassword:

PUT on to the local database for authentication.

Method	Request Body	Response Code	Response Body	Comment

PUT	{ **ConfirmPassword:** Enter the password of this administrator account. Range: 1 to 1024. **Name:** Enter the username of this administrator account. Administrator accounts enable people or external systems to access this system. This field is case sensitive. Range: 0 to 128. **Password:** Enter the password of this administrator account. Range: 1 to 1024. **YourCurrentPassword:** Enter your current password to authorize this change. Range: 1 to 1024. } **Required:** *Name, Password, ConfirmPassword, YourCurrentPassword*	200	{ **Message:** Success/Failure/Info message for the operation. }	Create an admin account password.

/common/certs/sch:

Read or update the Smart Call Home (SCH) server certificate resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	Certificate content.	Get the Smart Call Home server certificate from its path.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **file:** file to upload. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Write the Smart Call Home server certificate to its path. The request body contains the SCH server certificate data.

/common/credential:

Create, read, update or delete credentials.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Name:** The list of usernames used by the Expressway when authenticating with another system. Range: 1 to 1024 characters. }	Read locally authenticated names of neighbors.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **Name:** The name required for entry in the local authentication database. Range: 1 to 1024 characters. **Password:** The password required for this entry in the local authentication database. The maximum plain text length is 128 characters, which will then be encrypted. } ***Required:*** *Name, Password.*	200	{ **Message:** Success/Failure/Info message for the operations. }	Adds a new credential.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **Name:** The username used by the Expressway when authenticating with another system. Range: 1 to 1024 characters. **NewName:** Change the existing credential name to another name. Range: 1 to 1024 characters. **Password:** Change password of the existing credential. The maximum plaintext length is 128 characters, which is then encrypted. } ***Required:*** *Name.*	200	{ **Message:** Success/Failure/Info message for the operations. }	Update either name, password or both for an existing credential.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** The name of the credential to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete a credential.

/common/current/active/firewallrules:

Get the active firewall rules.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **action:** The action to take against any IP traffic that matches the rule. **address:** Determine the IP addresses to which the rule applies. Maximum: 1024. Minimum: 1. **description:** An optional free-form description of the firewall rule. Range 0 to 255 characters. **end_port:** The upper port in the range to which the rule applies. Maximum: 65535. Minimum: 0. **interface:** The LAN interface on which you want to control access. Default: LAN1. **prefix_length:** The field determines the range of the range of IP adresses to which the rule applies. Maximum: 128. Minimum: 0. **priority:** The order in which the firewall rules are applied. Maximum: 65534. Minimum: 1. **service:** The service to which the rule applies, or choose Custom to specify your own transport type and port ranges. **start_port:** The lower port in the range to which the rule applies. Maximum: 65535. Minimum: 0. **transport:** The transport protocol to which the rule applies. }	Get the active firewall rules present.

/common/defaultlinks:

Check or create the default links.

Method	Request Body	Response Code	Response Body	Comment
POST	DefaultLinksAdd	200	{ **Message:** Success/Failure/Info message for the operation. }	Performs the DefaultLinksAdd operation, which checks for the system-created default links and returns a status OK. Creates the default links if deleted and returns status.

/common/dns/dns:

Update or read the Domain Name System (DNS) data.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **DNSRequestsPortRange:** Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure. Default: EphemeralPortRange. **DNSRequestsPortRangeEnd:** The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 65534. **DNSRequestsPortRangeStart:** The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 1024. **DomainName:** The name to be appended to an unqualified host name before querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. May also be used along with the local System host name to identify references to this system in SIP messaging. **SystemHostName:** Defines the DNS hostname that this system is known by. Note that this is not the Fully Qualified Domain Name, just the host label portion. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit. Range 0 to 63 characters. }	Reads the DNS data.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **DNSRequestsPortRange:** Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure. Default: EphemeralPortRange. **DNSRequestsPortRangeEnd:** The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 65534. **DNSRequestsPortRangeStart:** The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 1024. **DomainName:** The name to be appended to an unqualified host name before querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. May also be used along with the local System host name to identify references to this system in SIP messaging. **SystemHostName:** Defines the DNS hostname that this system is known by. Note that this is not the Fully Qualified Domain Name, just the host label portion. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit. Range 0 to 63 characters. }	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the DNS data.

/common/dns/dnsperdomainserver:

Create, read, update or delete the per domain DNS server information.

Method	Request Body	Response Code	Response Body	Comment
GET	None	201	{ **address:** The IP address of the DNS server to use only when resolving hostnames for the associated domain names. Range: 1 to 1024 characters. **domain1:** The domain names to be resolved by this particular DNS server. You can specify either 1 or 2 domain names. Range: 1 to 1024 characters. **domain2:** The domain names to be resolved by this particular DNS server. You can specify either 1 or 2 domain names. Range: 1 to 1024 characters. **index:** Index is a priority parameter for the DNS server. Range 1 to 5. }	Read the per domain DNS server.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **address:** The IP address of the DNS server to use only when resolving hostnames for the associated domain names. Range: 1 to 1024 characters. **domain1:** The domain names to be resolved by this particular DNS server. You can specify either 1 or 2 domain names. Range: 1 to 1024 characters. **domain2:** The domain names to be resolved by this particular DNS server. You can specify either 1 or 2 domain names. Range: 1 to 1024 characters. **index:** Index is a priority parameter for the DNS server. Range 1 to 5. }	200	{ **Message:** Success/Failure/ Info message for the operation. }	Update the per domain DNS server.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **address:** The IP address of the DNS server to use only when resolving hostnames for the associated domain names. Range: 1 to 1024 characters. **domain1:** The domain names to be resolved by this particular DNS server. You can specify either 1 or 2 domain names. Range: 1 to 1024 characters. **domain2:** The domain names to be resolved by this particular DNS server. You can specify either 1 or 2 domain names. Range: 1 to 1024 characters. **index:** Index is a priority parameter for the DNS server. Range 1 to 5. }	200	{ **Message:** Success/Failure/ Info message for the operations. }	Update the per domain DNS server.

Method	Request Body	Response Code	Response Body	Comment
DELETE	**index:** Index is a priority parameter for the DNS server.	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete the DNS per domain server provided in the input data.

/common/dns/dnsserver:

Create, read, update or delete the Domain Name System (DNS) server information

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **address:** The IP address of a default DNS server to use when resolving domain names. You can specify up to 5 servers. The API will update/create one server at a time. The default DNS servers are used if there is no per-domain DNS server defined for the domain being looked up. Range 1 to 1024 characters. **index:** Index is a priority parameter for the DNS server. }	Read the DNS server data from the CDB.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **address:** The IP address of a default DNS server to use when resolving domain names. You can specify up to 5 servers. The API will update/create one server at a time. The default DNS servers are used if there is no per-domain DNS server defined for the domain being looked up. Range 1 to 1024 characters. **index:** Index is a priority parameter for the DNS server. }	201	{ **Message:** Success/Failure/ Info message for the operation. }	Create the per domain DNS server.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **address:** The IP address of a default DNS server to use when resolving domain names. You can specify up to 5 servers. The API will update/create one server at a time. The default DNS servers are used if there is no per-domain DNS server defined for the domain being looked up. Range 1 to 1024 characters. **index:** Index is a priority parameter for the DNS server. }	200	{ **Message:** Success/Failure/ Info message for the operations. }	Update the DNS server data.

Method	Request Body	Response Code	Response Body	Comment
DELETE	**index:** Index is a priority parameter for the DNS server	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete the DNS server provided.

/common/domain:

Create, read or update the domain configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	201	{ **EdgeSip:** Service status of EdgeSIP domain. Endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified CM gateway to provide secure firewall traversal and line-side support for Cisco Unified Communications Manager registrations. **EdgeXmpp:** Service status of the XMPP domain. Cisco Unified Communications Manager IM and Presence Service provides instant messaging and presence services for this SIP domain. **Index:** The index value of the domain. Range 1 to 200 characters. **Name:** The name of the domain managed by this Expressway. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters. **XmppFederation:** Indicates that XMPP federated services will be provided for this local domain. Note that if static routes for federated foreign domains are required, you can configure them on the Cisco Expressway-E. }	Read the domain and its other related information.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **EdgeSip:** Endpoint registration, call control and provisioning for this SIP domain is serviced by Cisco Unified Communications Manager. The Expressway acts as a Cisco Unified Communications Manager gateway to provide secure firewall traversal and line-side support for Cisco Unified Communications Manager registrations. **EdgeXmpp:**Cisco Unified Communications Manager IM and Presence Service provides instant messaging and presence services for this SIP domain. **XmppFederation:** Indicates that XMPP federated services will be provided for this local domain. Note that if static routes for federated foreign domains are required, you can configure them on the Cisco Expressway-E. **Name:** The name of the domain managed by this Expressway. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters. }	201	{ **Message:** Success /Failure/Info message for the operations. }	Add a domain.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **EdgeSip:** Endpoint registration, call control and provisioning for this SIP domain is serviced by Cisco Unified Communications Manager. The Expressway acts as a Cisco Unified Communications Manager gateway to provide secure firewall traversal and line-side support for Cisco Unified Communications Manager registrations. **EdgeXmpp:**Cisco Unified Communications Manager IM and Presence Service provides instant messaging and presence services for this SIP domain. **XmppFederation:** Indicates that XMPP federated services will be provided for this local domain. Note that if static routes for federated foreign domains are required, you can configure them on the Cisco Expressway-E. **Name:** The name of domain. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters. **NewName:** The name of the new domain. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters. }	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the domain.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** Name of the domain to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/Failure/Info message for the operations }	Delete the domain.

/common/firewallrules/activation:

Activate a firewall rules.

Method	Request Body	Response Code	Response Body	Comment
PUT				Activate firewall rules.

/common/firewallrules/configuration:

CRUD for firewall rules.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **action:** The action to take against any IP traffic that matches the rule. **address:** Determine the IP addresses to which the rule applies. Range 1 to 1024. **description:** An optional free-form description of the firewall rule. Range 0 to 255. **end_port:** The upper port in the range to which the rule applies. Range 0 to 65525. **index:** The unique ID of the firewall rule. **interface:** The LAN interface on which you want to control access. Default: LAN1. }**prefix_length:** The field determines the range of the range of IP adresses to which the rule applies. Range 1 to 6554. **priority:** The order in which the firewall rules are applied. **service:** The service to which the rule applies, or choose Custom to specify your own transport type and port ranges. **start_port:** The lower port in the range to which the rule applies. Range 0 to 65535. **transport:** The transport protocol to which the rule applies. }	Gets the firewall rules present.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **action:** The action to take against any IP traffic that matches the rule. **address:** Determine the IP addresses to which the rule applies. Range 1 to 1024. **description:** An optional free-form description of the firewall rule. Range 0 to 255. **end_port:** The upper port in the range to which the rule applies. Range 0 to 65525. **index:** The unique ID of the firewall rule. **interface:** The LAN interface on which you want to control access. Default: LAN1. **prefix_length:** The field determines the range of the range of IP adresses to which the rule applies. Range 0 to 128. **priority:** The order in which the firewall rules are applied. Range: 1 to 65534. **service:** The service to which the rule applies, or choose Custom to specify your own transport type and port ranges. **start_port:** The lower port in the range to which the rule applies. Range: 0 to 65535. **transport:** The transport protocol to which the rule applies. }	200	{ **Message:** Success/Failure/Info message for the operations. }	Create a firewall rule configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **action:** The action to take against any IP traffic that matches the rule. **address:** Determine the IP addresses to which the rule applies. Range 1 to 1024. **description:** An optional free-form description of the firewall rule. Range 0 to 255. **end_port:** The upper port in the range to which the rule applies. Range 0 to 65525. **index:** The unique ID of the firewall rule. **interface:** The LAN interface on which you want to control access. Default: LAN1. }**prefix_length:** The field determines the range of the range of IP adresses to which the rule applies. Range 0 to 128. **priority:** The order in which the firewall rules are applied. Range: 1 to 65534. **service:** The service to which the rule applies, or choose Custom to specify your own transport type and port ranges. **start_port:** The lower port in the range to which the rule applies. Range: 0 to 65535. **transport:** The transport protocol to which the rule applies. }	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the firewall rules.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **index:** The unique ID of the firewall rule. } ***Required:*** *index.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete a firewall rule configuration.

/common/mra:

Update or read the current Mobile and Remote Access (MRA) configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Enabled:** Enable or disable Mobile and Remote Access (MRA). MRA allows endpoints such as Cisco Jabber to have their registration, call control, messaging and provisioning services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations. **IOSSafariPlugin:** IOS Cisco Jabber client using Safari plugin. **SSO:** Control SSO access. **SSODefaulted:** Default SSO availability. } ***Required:*** *Enabled.*	Read the MRA configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **Enabled:** Enable or disable Mobile and Remote Access (MRA). MRA allows endpoints such as Cisco Jabber to have their registration, call control, messaging and provisioning services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations. **IOSSafariPlugin:** IOS Cisco Jabber client using Safari plugin. **SSO:** Control SSO access. **SSODefaulted:** Default SSO availability. } ***Required:*** *Enabled.*	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Update the MRA configuration.

/common/protocol/sip:

CRUD operations for SIP STATUS Rest API.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AllowCrlDownloadsFromCdps:** Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. Default: Yes. **CertRevocationCheckMode:** Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. Default: On. **FallbackBehavior:** Controls the revocation checking behavior. Default: TreatAsNotRevoked. **IPv4Mtls:** status of IPv4 MTLS port. **IPv4Tcp:** status of IPv4 TCP port. **IPv4TcpAddress:** IPv4 TCP address. **IPv4Tls:** status of IPv4 TLS port. **IPv4TlsAddress:** IPv4 TLS address. **IPv4Udp:** status of IPv4 UDP port. **IPv4UdpAddress:** IPv4 UDP address. **iPv6Mtls:** status of IPv6 MTLS port. **IPv6Tcp:** status of IPv6 TCP port. **IPv6Tls:** status of IPv6 TLS port. **IPv6Udp:** status of IPv4 UDP port. **MinSessionRefreshInterval:** Switch Mutual TLS mode on to enable a separate port to enforce Mutual TLS authentication on incoming SIP calls to this Expressway. Default: Off. **MutualTlsPort:** The listening port for incoming SIP Mutual TLS calls. Default: 5062. **OutRegRefreshMax:** The maximum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the Outbound registration refresh strategy). Default: 3600. Range: 30 to 7200. **OutRegRefreshMin:** The minimum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. Default: 600. Range 30 to 3600.	Get the SIP configuration.

Method	Request Body	Response Code	Response Body	Comment
			OutRegRefreshStrategy: Method used to generate the SIP registration expiry period for Outbound registrations. The registration expiry period is the period within which a SIP endpoint must re-register to prevent its registration expiring. Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration. Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration. Default: Variable. **SdpMaxSize:** Specifies the maximum size of SDP payload that can be handled by the server (in bytes). Default: 32768. Range: 1 to 65536. **SessionRefreshInterval:** The maximum time allowed between session refresh requests for SIP calls. Default: 1800. Range 90 to 84600. **SessionRefreshInterval:** The maximum time allowed between session refresh requests for SIP calls. Default: 1800. Range 90 to 84600. **SipMode:** "Determines whether or not the Expressway will provide SIP registrar and SIP proxy functionality.This mode must be enabled in order to use either the Presence Server or the Presence User Agent. Default: Off. **SipRegProxyMode:** Specifies how the Expressway handles registration requests for domains for which it is not acting as a SIP registrar (non-local domains). Off: registration requests are not proxied. Proxy to known only: registration requests are proxied in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones. Proxy to any: registration requests are proxied in accordance with existing call processing rules to all known zones. Default: Off. **SipTcpConnectTimeout:** Specifies the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default: 10. Range: 1 to 150. **StdRegRefreshMax:** The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the standard registration refresh strategy). Default: 60. Range: 30 to 7200. **StdRegRefreshMin:** The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. Default: 45. Range: 30 to 3600.	

Method	Request Body	Response Code	Response Body	Comment

			StdRegRefreshStrategy: Method used to generate the SIP registration expiry period for standard registrations. The registration expiry period is the period within which a SIP endpoint must re-register to prevent its registration expiring. Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration. Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration. Default: Maximum. **TcpMode:** Determines whether incoming and outgoing SIP messages using the TCP protocol are allowed. Default: Off. **TcpOutboundPortEnd:** Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections. Default: 29999. Range: 1024 to 65534. **TcpOutboundPortStart:** Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections. Default: 25000. Range: 1024 to 65534. **TcpPort:** The listening port for incoming SIP TCP connections. Default: 5060. Range 1024 to 65534. **TlsHandshakeTimeout:** Specifies the timeout period for TLS socket handshake in seconds. Default: 5. Range: 1 to 120. **TlsMode:** Determines whether incoming and outgoing SIP messages using the TLS protocol are allowed. Default: On. **TlsPort:** The listening port for incoming SIP TLS connections. Default: 5061. Range: 1024 to 65534. **UdpMode:** Determines whether incoming and outgoing SIP messages using the UDP protocol are allowed. Default: On. **UdpPort:** The listening port for incoming SIP UDP messages. Default: 5060. Range: 1024 to 65534. **UseCrl:** Controls whether the Certificate Revocation Lists (CRLs) may be used to perform certificate revocation checking. Default: Yes. **UseOcsp:** Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking. Default: Yes. **Required:** UdpPort, MutualTlsMode, TlsMode, TcpMode, UdpMode, SipMode, TcpPort, SessionRefreshInterval, TlsHandshakeTimeout, TcpOutboundPortEnd, TlsPort, MutualTlsPort, TcpOutboundPortStart, MinSessionRefreshInterval, CertRevocationCheckMode, OutRegRefreshStrategy, SipRegProxyMode, StdRegRefreshStrategy, StdRegRefreshMin, OutRegRefreshMin, StdRegRefreshMax, OutRegRefreshMax, SdpMaxSize, SipTcpConnectTimeout }	

/common/protocol/sip/advanced:

CRUD operations for SIP Advanced Rest API.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **SdpMaxSize:** Specifies the maximum size of SDP payload that can be handled by the server (in bytes). Default: 32768. Range 1 to 65536. **SipTcpConnectTimeout:** Specifies the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default: 10. Range 1 to 150. }	Gets the SIP advanced configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **SdpMaxSize:** Specifies the maximum size of SDP payload that can be handled by the server (in bytes). Default: 32768. Range: 1 to 65536. **SipTcpConnectTimeout:** Specifies the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default: 10. Range: 1 to 150. }	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the SIP advanced configuration.

/common/protocol/sip/certrevokecheck:

CRUD operations for SIP Certification Revoke Check Rest API.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AllowCrlDownloadsFromCdps:** Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. Default: Yes. **CertRevocationCheckMode:** Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. Default: On. **FallbackBehavior:** Controls the revocation checking behavior. Default: TreatAsNotRevoked. **UseCrl:** Controls whether the Certificate Revocation Lists (CRLs) may be used to perform certificate revocation checking. Default: Yes. **UseOcsp:** Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking. Default: Yes. }	Gets the SIP Certification Revoke Check.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AllowCrlDownloadsFromCdps:** Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. Default: Yes. **CertRevocationCheckMode:** Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. Default: On. **FallbackBehavior:** Controls the revocation checking behavior. Default: TreatAsNotRevoked. **UseCrl:** Controls whether the Certificate Revocation Lists (CRLs) may be used to perform certificate revocation checking. Default: Yes. **UseOcsp:** Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking. Default: Yes. }	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the SIP configuration.

/common/protocol/sip/configuration:

CRUD operations for SIP Configuration Rest API.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **MinSessionRefreshInterval:** The minimum value the VCS will negotiate for the session refresh interval for SIP calls. Default: 500. Range: 90 to 84600. **MutualTlsMode:** Switch Mutual TLS mode on to enable a separate port to enforce Mutual TLS authentication on incoming SIP calls to this Expressway. Default: Off. **MutualTlsPort:** The listening port for incoming SIP Mutual TLS calls. Default: 5062. Range: 90 to 84600. **SessionRefreshInterval:** The maximum time allowed between session refresh requests for SIP calls. Default: 1800. Range: 90 to 84600. **SipMode:** Determines whether or not the Expressway will provide SIP registrar and SIP proxy functionality. This mode must be enabled in order to use either the Presence Server or the Presence User Agent. Default: Off. **TcpMode:** Determines whether incoming and outgoing SIP messages using the TCP protocol are allowed. Default: Off. **TcpOutboundPortEnd:** Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections. Default: 29999. Range: 1024 to 65534. **TcpOutboundPortStart:** Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections. Default: 2500. Range: 1024 to 65534. **TcpPort:** The listening port for incoming SIP TCP connections. Default: 5060. Range: 1024 to 65534. **TlsHandshakeTimeout:** Specifies the timeout period for TLS socket handshake in seconds. Default: 5. Range: 1 to 120. **TlsMode:** Determines whether incoming and outgoing SIP messages using the TLS protocol are allowed. Default: On. **TlsPort:** The listening port for incoming SIP TLS connections. Default: 5061. Range: 1024 to 65534. **UdpMode:** Determines whether incoming and outgoing SIP messages using the UDP protocol are allowed. Default: On. **UdpPort:** The listening port for incoming SIP UDP messages. Default: 5060. Range: 1024 to 65534. }	Gets the SIP advanced configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **MinSessionRefreshInterval:** The minimum value the VCS will negotiate for the session refresh interval for SIP calls. Default: 500. Range: 90 to 84600. **MutualTlsMode:** Switch Mutual TLS mode on to enable a separate port to enforce Mutual TLS authentication on incoming SIP calls to this Expressway. Default: Off. **MutualTlsPort:** The listening port for incoming SIP Mutual TLS calls. Default: 5062. Range: 90 to 84600. **SessionRefreshInterval:** The maximum time allowed between session refresh requests for SIP calls. Default: 1800. Range: 90 to 84600. **SipMode:** Determines whether or not the Expressway will provide SIP registrar and SIP proxy functionality. This mode must be enabled in order to use either the Presence Server or the Presence User Agent. Default: Off. **TcpMode:** Determines whether incoming and outgoing SIP messages using the TCP protocol are allowed. Default: Off. **TcpOutboundPortEnd:** Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections. Default: 29999. Range: 1024 to 65534. **TcpOutboundPortStart:** Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections. Default: 2500. Range: 1024 to 65534. **TcpPort:** The listening port for incoming SIP TCP connections. Default: 5060. Range: 1024 to 65534 **TlsHandshakeTimeout:** Specifies the timeout period for TLS socket handshake in seconds. Default: 5. Range: 1 to 120. **TlsMode:** Determines whether incoming and outgoing SIP messages using the TLS protocol are allowed. Default: On. **TlsPort:** The listening port for incoming SIP TLS connections. Default: 5061. Maximum: 65534. Minimum: 1024. Range: 1024 to 65534. **UdpMode:** Determines whether incoming and outgoing SIP messages using the UDP protocol are allowed. Default: On. **UdpPort:** The listening port for incoming SIP UDP messages. Default: 5060. Range: 1024 to 65534 }	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the SIP advanced configuration.

/common/protocol/sip/registrationcontrol:

CRUD operations for SIP Registration Control Rest API.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **OutRegRefreshMax:** The maximum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the Outbound registration refresh strategy). Default: 3600. Range 30 to 7200. **OutRegRefreshMin:** The minimum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. Default: 600. Range: 30 to 3600. **OutRegRefreshStrategy:** Method used to generate the SIP registration expiry period for Outbound registrations. The registration expiry period is the period within which a SIP endpoint must re-register to prevent its registration expiring. Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration. Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration. Default: Variable. **SipRegProxyMode:** Specifies how the Expressway handles registration requests for domains for which it is not acting as a SIP registrar (non-local domains). Off: registration requests are not proxied. Proxy to known only: registration requests are proxied in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones. Proxy to any: registration requests are proxied in accordance with existing call processing rules to all known zones. Default: Off. **StdRegRefreshMax:** The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the standard registration refresh strategy). Default: 60. Range: 30 to 3600.	Get the SIP registration control.

Method	Request Body	Response Code	Response Body	Comment
			std_reg_refresh_min: The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. Default: 45. Range: 30 to 3600. **std_reg_refresh_strategy:** Method used to generate the SIP registration expiry period for standard registrations. The registration expiry period is the period within which a SIP endpoint must re-register to prevent its registration expiring. Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration. Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration. Default: Maximum. }	

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **out_reg_refresh_max:** The maximum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the Outbound registration refresh strategy). Default: 3600. Range: 30 to 3600. **out_reg_refresh_min:** The minimum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. Default: 600. Range: 30 to 3600. **out_reg_refresh_strategy:** Method used to generate the SIP registration expiry period for Outbound registrations. The registration expiry period is the period within which a SIP endpoint must re-register to prevent its registration expiring. Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration. Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration. Default: Variable. **sip_reg_proxy_mode:** Specifies how the Expressway handles registration requests for domains for which it is not acting as a SIP registrar (non-local domains). Off: registration requests are not proxied. Proxy to known only: registration requests are proxied in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones. Proxy to any: registration requests are proxied in accordance with existing call processing rules to all known zones. Default: Off.	200	{ **Message:** Success/Failure/Info message for the operations. }	Update the SIP registration control.

Method	Request Body	Response Code	Response Body	Comment
	std_reg_refresh_max: The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the standard registration refresh strategy). Default: 60. Range: 30 to 3600. **std_reg_refresh_min:** The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. Default: 45. Range: 30 to 3600. **std_reg_refresh_strategy:** Method used to generate the SIP registration expiry period for standard registrations. The registration expiry period is the period within which a SIP endpoint must re-register to prevent its registration expiring. Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration. Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration. Default: Maximum. }			

/common/qos:

Read or update the current Quality of Service(QoS) configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Audio:** The DSCP value to be stamped onto SIP and H.323 audio media traffic routed through the Expressway. Note: you must restart the system for any changes to take effect. Default: 46. Range 0 to 63. **Signaling:** The DSCP value to be stamped onto all SIP and H.323 signaling traffic routed through the Expressway. Note: you must restart the system for any changes to take effect. Default: 24. Range 0 to 63. **Video:** The DSCP value to be stamped onto SIP and H.323 video media traffic routed through theExpressway. Note: you must restart the system for any changes to take effect. Default: 34. Range 0 to 63. **XMPP:** The DSCP value to be stamped onto XMPP traffic routed through theExpressway. Note: you must restart the system for any changes to take effect. Default: 24. Range 0 to 63. }	Read the QoS configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **Audio:** The DSCP value to be stamped onto SIP and H.323 audio media traffic routed through the Expressway. Note: you must restart the system for any changes to take effect. Default: 46. Range 0 to 63. **Signaling:** The DSCP value to be stamped onto all SIP and H.323 signaling traffic routed through the Expressway. Note: you must restart the system for any changes to take effect. Default: 24. Range 0 to 63. **Video:** The DSCP value to be stamped onto SIP and H.323 video media traffic routed through theExpressway. Note: you must restart the system for any changes to take effect. Default: 34. Range 0 to 63. **XMPP:** The DSCP value to be stamped onto XMPP traffic routed through theExpressway. Note: you must restart the system for any changes to take effect. Default: 24. Range 0 to 63. }	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Update QoS configuration.

/common/sch:

Update or get the Smart Call Home configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **ContactEmail:** Contact email address. Range 1 to 1024 characters. **ContactName:** Contact name. Range 1 to 1024 characters. **ContactTelephone:** Contact telephone number. Range 1 to 1024 characters. **Message:** Smart Call Home final configuration message. Range 1 to 1024 characters. **OrganizationAddress:** Address of the organization. Range 1 to 1024 characters. **OrganizationName:** Name of the organization. Range 1 to 1024 characters. **SmartCallHome:** Smart Call Home mode. }	Reads the Smart Call Home configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **ContactEmail:** Contact email address. Range 1 to 1024 characters. **ContactName:** Contact name. Range 1 to 1024 characters. **ContactTelephone:** Contact telephone number. Range 1 to 1024 characters. **Message:** Smart Call Home Final configuration message. Range 1 to 1024 characters. **OrganizationAddress:** Address of the organization. Range 1 to 1024 characters. **OrganizationName:** Name of the organization. Range 1 to 1024 characters. **SmartCallHome:** Smart Call Home mode. **SmartCallHome:** Select your preferred Smart Call Home mode. Off: The Expressway does not call home. On: Turns on the Smart Call Home service. This option requires some contact details from you, so that we can alert you to issues that the Expressway reports to Smart Call Home. On (Anonymous): Turns on the Smart Call Home service in Anonymous mode. The Expressway still reports to Smart Call Home, but you do not receive notifications. }	200	{ **ContactEmail:** Contact email address. Range 1 to 1024 characters. **ContactName:** Contact name. Range 1 to 1024 characters. **ContactTelephone:** Contact telephone number. Range 1 to 1024 characters. **Message:** Smart Call Home final configuration message. Range 1 to 1024 characters. **OrganizationAddress:** Address of the organization. Range 1 to 1024 characters. **OrganizationName:** Name of the organization. Range 1 to 1024 characters. **SmartCallHome:** Smart Call Home mode. }	Updates the Smart Call Home configuration.

/common/searchrule:

Create, read, update or delete the search rule information.

Method	Request Body	Response Code	Response Body	Comment
GET	None	201	{ **Description:** A free-form description of the search rule. Range 0 to 64 characters. **Mode:** The type of alias for which this search rule applies. AliasPatternMatch: the alias must match the specified pattern type and string. AnyAlias: any alias (providing it is not an IP address) is allowed. AnyIPAddress: the alias must be an IP address. Default: AnyAlias. **MustAuthenticateRequest:** Specifies whether this search rule applies only to authenticated search requests. Default: No. **Name:** The name of the SearchRule. Range 0 to 50 characters. **OnSuccessfulMatch:** Specifies the ongoing search behavior if the alias matches all of the search rule's conditions. Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. Stop: any remaining search rules with a lower priority are not applied, even if the endpoint identified by the alias is ultimately not found. Default: Continue. **PatternBehavior:** Determines whether the matched part of the alias is modified before being sent to the target zone or policy service. (Applies to Alias Pattern Match mode only.) Leave: the alias is not modified. Strip: the matching prefix or suffix is removed from the alias. Replace: the matching part of the alias is substituted with the text in the replace string. Default: Strip. **PatternString:** The pattern against which the alias is compared. (Applies to Alias pattern match mode only.) Note: if the pattern string is a Regex, you can refer to the regular expressions reference table in the online help. **PatternType:** How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) Exact: the entire string must exactly match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string is treated as a regular expression. Default: Prefix.	Fetches (all / by name) the search rules defined along with their parameters.

Method	Request Body	Response Code	Response Body	Comment
			Priority: The order in the search process that this rule is applied, when compared to the priority of the other search rules. All priority 1 search rules are applied first, followed by all priority 2 search rules, and so on. Default 100. Range 1 to 65534. **Protocol:** The source protocol for which this rule applies. Default: Any. **ReplaceString:** The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only). Range 0 to 60. **SIPVariant:** Select which type of SIP messages this search rule will process. Choose MicrosoftAny if you want the search rule to route MicrosoftSIP and MicrosoftIMP. Choose Standard to ignore Microsoft types and route standards-compliant SIP, or choose Any to route all types. Default: Any. **Source:** The sources of the requests for which this rule applies. Any: locally registered devices, neighbor or traversal zones, and any non-registered devices. AllZones: locally registered devices plus neighbor or traversal zones. LocalZone: locally registered devices only. Named: a specific zone or subzone. Default: Any. **SourceName:** The specific source zone or subzone for which this rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone. **State:** Indicates if the search rule is enabled or disabled. Disabled search rules are ignored. Default: Enabled. **SystemGenerated:** The status of the zone. **TargetName:** The zone name or policy service name to query if the alias matches the search rule. Range 1 to 60. } ***Required:*** *SIPVariant, Protocol, Name, ReplaceString, OnSuccessfulMatch, SourceName, TargetName, PatternString, State, Priority, Source, PatternType, Mode, PatternBehavior, MustAuthenticateRequest.*	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **Description:** A free-form description of the search rule. Range 0 to 64 characters. **Mode:** The type of alias for which this search rule applies. AliasPatternMatch: the alias must match the specified pattern type and string. AnyAlias: any alias (providing it is not an IP address) is allowed. AnyIPAddress: the alias must be an IP address. Default: AnyAlias. **MustAuthenticateRequest:** Specifies whether this search rule applies only to authenticated search requests. Default: No. **Name:** The name of the SearchRule. Range 0 to 50 characters. **OnSuccessfulMatch:** Specifies the ongoing search behavior if the alias matches all of the search rule's conditions. Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. Stop: any remaining search rules with a lower priority are not applied, even if the endpoint identified by the alias is ultimately not found. Default: Continue. **PatternBehavior:** Determines whether the matched part of the alias is modified before being sent to the target zone or policy service. (Applies to Alias Pattern Match mode only.) Leave: the alias is not modified. Strip: the matching prefix or suffix is removed from the alias. Replace: the matching part of the alias is substituted with the text in the replace string. Default: Strip. **PatternString:** The pattern against which the alias is compared. (Applies to Alias pattern match mode only.) Note: if the pattern string is a Regex, you can refer to the regular expressions reference table in the online help. **PatternType:** How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) Exact: the entire string must exactly match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string is treated as a regular expression. Default: Prefix.	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Create a new search rule.

Method	Request Body	Response Code	Response Body	Comment
	Priority: The order in the search process that this rule is applied, when compared to the priority of the other search rules. All priority 1 search rules are applied first, followed by all priority 2 search rules, and so on. Default 100. Range 1 to 65534. **Protocol:** The source protocol for which the rule applies. Default: Any. **ReplaceString:** The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only). Range 0 to 60. **SIPVariant:** Select which type of SIP messages this search rule will process. Choose MicrosoftAny if you want the search rule to route MicrosoftSIP and MicrosoftIMP. Choose Standard to ignore Microsoft types and route standards-compliant SIP, or choose Any to route all types. Default: Any. **Source:** The sources of the requests for which this rule applies. Any: locally registered devices, neighbor or traversal zones, and any non-registered devices. AllZones: locally registered devices plus neighbor or traversal zones. LocalZone: locally registered devices only. Named: a specific zone or subzone. Default: Any. **SourceName:** The specific source zone or subzone for which this rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone. **State:** Indicates if the search rule is enabled or disabled. Disabled search rules are ignored. Default: Enabled. **TargetName:** The zone name or policy service name to query if the alias matches the search rule. Range 1 to 60. } ***Required:*** *Name, Priority, TargetName.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	**Description:** A free-form description of the search rule. Range 0 to 64 characters. **Mode:** The type of alias for which this search rule applies. AliasPatternMatch: the alias must match the specified pattern type and string. AnyAlias: any alias (providing it is not an IP address) is allowed. AnyIPAddress: the alias must be an IP address. Default: AnyAlias. **MustAuthenticateRequest:** Specifies whether this search rule applies only to authenticated search requests. Default: No. **Name:** The name of the SearchRule. Range 0 to 50 characters. **NewName:** The name of the SearchRule. Range 0 to 50 characters. **OnSuccessfulMatch:** Specifies the ongoing search behavior if the alias matches all of the search rule's conditions. Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. Stop: any remaining search rules with a lower priority are not applied, even if the endpoint identified by the alias is ultimately not found. Default: Continue. **PatternBehavior:** Determines whether the matched part of the alias is modified before being sent to the target zone or policy service. (Applies to Alias Pattern Match mode only.) Leave: the alias is not modified. Strip: the matching prefix or suffix is removed. from the alias. Replace: the matching part of the alias is substituted with the text in the replace string. Default: Strip. **PatternString:** The pattern against which the alias is compared. (Applies to Alias pattern match mode only.) Note: if the pattern string is a Regex, you can refer to the regular expressions reference table in the online help. **PatternType:** How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) Exact: the entire string must exactly match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string is treated as a regular expression. Default: Prefix.	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Update the configuration of an existing search rule

Method	Request Body	Response Code	Response Body	Comment
	Priority: The order in the search process that this rule is applied, when compared to the priority of the other search rules. All priority 1 search rules are applied first, followed by all priority 2 search rules, and so on. Default 100. Range 1 to 65534. **Protocol:** The source protocol for which this rule applies. Default: Any. **ReplaceString:** The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only). Range 0 to 60. **SIPVariant:** Select which type of SIP messages this search rule will process. Choose MicrosoftAny if you want the search rule to route MicrosoftSIP and MicrosoftIMP. Choose Standard to ignore Microsoft types and route standards-compliant SIP, or choose Any to route all types. Default: Any. **Source:** The sources of the requests for which this rule applies. Any: locally registered devices, neighbor or traversal zones, and any non-registered devices. AllZones: locally registered devices plus neighbor or traversal zones. LocalZone: locally registered devices only. Named: a specific zone or subzone. Default: Any. **SourceName:** The specific source zone or subzone for which this rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone. **State:** Indicates if the search rule is enabled or disabled. Disabled search rules are ignored. Default: Enabled. **TargetName:** The zone name or policy service name to query if the alias matches the search rule. Range 1 to 60. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** The name of the SearchRule. Range: 1 to 50. } Required: Name.	200	{ **Message:** Success/Failure/Info message for the operation. }	Deleting a search rule.

/common/time/ntpserver:

Read, update or delete the NTP server details.

Method	Request Body	Response Code	Response Body	Comment
GET	None.	200	{ **Address:** Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time. Range 1 to 1024. **Authentication:** The type of NTP server authentication to use. Disabled: no authentication is used. Symmetric key: uses key values entered here that must match exactly the equivalent settings on the NTP server. Private key: uses an automatically generated private key with which to authenticate messages sent to the NTP server. Default: disabled. **Hash:** The cryptographic hash type to use with NTP symmetric authentication. It must match the hash type for the specified key on the NTP server. Default: SHA-1. **KeyId:** The key identifier to use with NTP symmetric authentication. It must match a trusted key on the NTP server. **PassPhrase:** The pass phrase to use with NTP symmetric authentication. It must match the pass phrase associated with the same key ID on the NTP server. Range 1 to 1024. **index:** The priority of the ntp server address. Range 1 to 5. } ***Required:*** *Address, Authentication, KeyId, Hash, index.*	Fetches all NTP server details defined.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **Address:** Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time. Range 1 to 1024. **Authentication:** The type of NTP server authentication to use. Disabled: no authentication is used. Symmetric key: uses key values entered here that must match exactly the equivalent settings on the NTP server. Private key: uses an automatically generated private key with which to authenticate messages sent to the NTP server. Default: disabled. **Hash:** The cryptographic hash type to use with NTP symmetric authentication. It must match the hash type for the specified key on the NTP server. Default: SHA-1. **KeyId:** The key identifier to use with NTP symmetric authentication. It must match a trusted key on the NTP server. **PassPhrase:** The pass phrase to use with NTP symmetric authentication. It must match the pass phrase associated with the same key ID on the NTP server. Range 1 to 1024. **index:** The priority of the ntp server address. Range 1 to 5. } ***Required:*** *Address, index.*	201	{ **Message:** Success/Failure/ Info message for the operation. }	Creates a NTP server address entry.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **Address:** Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time. Range 1 to 1024. **Authentication:** The type of NTP server authentication to use. Disabled: no authentication is used. Symmetric key: uses key values entered here that must match exactly the equivalent settings on the NTP server. Private key: uses an automatically generated private key with which to authenticate messages sent to the NTP server. Default: disabled. **Hash:** The cryptographic hash type to use with NTP symmetric authentication. It must match the hash type for the specified key on the NTP server. Default: SHA-1. **KeyId:** The key identifier to use with NTP symmetric authentication. It must match a trusted key on the NTP server. **PassPhrase:** The pass phrase to use with NTP symmetric authentication. It must match the pass phrase associated with the same key ID on the NTP server. Range 1 to 1024. **index:** The priority of the ntp server address. Range 1 to 5. } ***Required:*** *Address, index.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Updates the NTP server details.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **index:** The priority of the ntp server address. } ***Required:*** *index.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Deletes the NTP server record.

/common/time/status:

Read the time status.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ NTP server status details. }	Fetches all NTP server status details.

/common/time/timezone:

Read or update the time zone.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **TimeZone:** Sets the local time zone of the system. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York. Default UTC. } ***Required:*** *TimeZone.*	Fetches the timezone details defined.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **TimeZone:** Sets the local time zone of the system. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York. Default UTC. } ***Required:*** *TimeZone.*	200	{ **Message:** Success/Failure/ Info message for the operation. }	Fetches the timezone details defined.

/common/transform:

Create, read, update or delete transforms.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Description:** A free-form description of the transform. **PatternBehavior:** How the alias is modified. Strip: removes the matching prefix or suffix from the alias. Replace: substitutes the matching part of the alias with the text in the replace string. AddPrefix: prepends the Additional text to the alias. AddSuffix: appends the Additional text to the alias. Default: Strip. **PatternReplaceString:** The text string to use in conjunction with the selected Pattern behavior. **PatternString:** The pattern against which the alias is compared. **PatternType:** How the pattern string must match the alias for the transform to be applied. Exact: the entire string must exactly match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string is treated as a regular expression. Default: Prefix. **Priority:** Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1. **State:** Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled. } ***Required:*** *PatternType, PatternReplaceString, PatternString, Priority, State, PatternBehavior, Description.*	Fetches (all / by Priority) transforms defined along with their parameters.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **Description:** A free-form description of the transform. **PatternBehavior:** How the alias is modified. Strip: removes the matching prefix or suffix from the alias. Replace: substitutes the matching part of the alias with the text in the replace string. AddPrefix: prepends the Additional text to the alias. AddSuffix: appends the Additional text to the alias. Default: Strip. **PatternReplaceString:** The text string to use in conjunction with the selected Pattern behavior. **PatternString:** The pattern against which the alias is compared. **PatternType:** How the pattern string must match the alias for the transform to be applied. Exact: the entire string must exactly match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string is treated as a regular expression. Default: Prefix. **Priority:** Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1. **State:** Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled. } ***Required:*** *Priority, PatternString, PatternBehavior.*	201	{ **Message:** Success/ Failure/ Info message for the operation. }	Create a new transform.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **Description:** A free-form description of the transform. **NewPriority:** Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default:1. **PatternBehavior:** How the alias is modified. Strip: removes the matching prefix or suffix from the alias. Replace: substitutes the matching part of the alias with the text in the replace string. AddPrefix: prepends the Additional text to the alias. AddSuffix: appends the Additional text to the alias. Default: Strip. **PatternReplaceString:** The text string to use in conjunction with the selected Pattern behavior. **PatternString:** The pattern against which the alias is compared. **PatternType:** How the pattern string must match the alias for the transform to be applied. Exact: the entire string must exactly match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string is treated as a regular expression. Default: Prefix. **Priority:** Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1. **State:** Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled. } ***Required:*** *Priority.*	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Update the configuration of an existing transform.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Priority:** Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1. } ***Required:*** *Priority*	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Delete a transform.

/common/zone/dnszone:

Create, read, update or delete the DNS zone.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AutomaticallyRespondToSIPSearches:** Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Off: a SIP OPTIONS message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **HopCount:** Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15. **IncludeAddressRecord:** Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS records. On: theExpressway will query for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. Off: the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones. Default: Off. **Name:** Name of the zone. Range 1 to 50. **SIPAuthenticationTrustMode:** Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials. Default: Off. **SIPDomainToSearchFor:** Enter a FQDN to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected.	Gets the zone configuration details for DNS zone

Method	Request Body	Response Code	Response Body	Comment
			SIPFallbackTransportProtocol: Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used. Default: UDP. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPModifyDnsRequest:** Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services. Default: Off. **SIPParameterPreservationMode:** Determines whether theExpressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. On preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone are poisoned" such that if they are received by the local Expresswayagain they will be rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061.	

Method	Request Body	Response Code	Response Body	Comment
			SIPPreloadedSipRoutesSupport: Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPRecordRouteAddressType:** Controls whether the Cisco VCS uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP. **SIPTLSVerifyInboundMapping:** Switch Inbound TLS mapping On to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as CN or SAN), then the connection is not mapped to this zone. Switch Inbound TLS mapping Off to prevent the Expressway from attempting to map inbound TLS connections to this zone. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. **SIPTLSVerifySubjectName:** The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). **SIPUDPBFCPFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUDPIXFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. Off: INVITE requests are not modified. Default: Off. **SendEmptyINVITEFor InterworkedCalls:** Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. On: SIP INVITEs with no SDP are generated and sent to this neighbor. Off: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor. Default: On.	

Method	Request Body	Response Code	Response Body	Comment
			Status: Status of the zone. **ZoneProfile:** Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Default: Default. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AutomaticallyRespondToSIP Searches:** Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Off: a SIP OPTIONS message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **HopCount:** Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15. **IncludeAddressRecord:** Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS records. On: theExpressway will query for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. Off: the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones. Default: Off. **Name:** Name of the zone. Range 1 to 50. **SIPAuthenticationTrustMode:** Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials. Default: Off. **SIPDomainToSearchFor:** Enter a FQDN to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected. **SIPFallbackTransportProtocol:** Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used. Default: UDP.	201	{ **Message:** Success /Failure/ Info message for the operation. }	Create DNS zone.

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaEncryptionMode: Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPModifyDnsRequest:** Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services. Default: Off. **SIPParameterPreservationMode:** Determines whether theExpressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. On preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone are poisoned" such that if they are received by the local Expresswayagain they will be rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPRecordRouteAddressType:** Controls whether the Cisco VCS uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.			

Method	Request Body	Response Code	Response Body	Comment
	SIPTLSVerifyInboundMapping: Switch Inbound TLS mapping On to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as CN or SAN), then the connection is not mapped to this zone. Switch Inbound TLS mapping Off to prevent the Expressway from attempting to map inbound TLS connections to this zone. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. **SIPTLSVerifySubjectName:** The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). **SIPUDPBFCPFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUDPIXFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. Off: INVITE requests are not modified. Default: Off. **SendEmptyINVITEForInterworked Calls:** Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. On: SIP INVITEs with no SDP are generated and sent to this neighbor. Off: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor. Default: On. **Status:** Status of the zone. **ZoneProfile:** Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Default: Default. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AutomaticallyRespondToSIPSearches:** Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Off: a SIP OPTIONS message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **HopCount:** Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15. **IncludeAddressRecord:** Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS records. On: theExpressway will query for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. Off: the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones. Default: Off. **Name:** Name of the zone. Range 1 to 50. **NewName:** New name of the zone. Range 1 to 50. **SIPAuthenticationTrustMode:** Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials. Default: Off. **SIPDomainToSearchFor:** Enter a FQDN to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected. **SIPFallbackTransportProtocol:** Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used. Default: UDP.	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Create DNS zone.

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaEncryptionMode: Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPModifyDnsRequest:** Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services. Default: Off. **SIPParameterPreservationMode:** Determines whether theExpressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. On preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone are poisoned" such that if they are received by the local Expresswayagain they will be rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPRecordRouteAddressType:** Controls whether the Cisco VCS uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.			

Method	Request Body	Response Code	Response Body	Comment
	SIPTLSVerifyInboundMapping: Switch Inbound TLS mapping On to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as CN or SAN), then the connection is not mapped to this zone. Switch Inbound TLS mapping Off to prevent the Expressway from attempting to map inbound TLS connections to this zone. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. **SIPTLSVerifySubjectName:** The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). **SIPUDPBFCPFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUDPIXFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. Off: INVITE requests are not modified. Default: Off. **SendEmptyINVITEForInterworked Calls:** Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. On: SIP INVITEs with no SDP are generated and sent to this neighbor. Off: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor. Default: On. **Status:** Status of the zone. **ZoneProfile:** Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Default: Default. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** The name of the zone to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Deleting the DNS zone.

/common/zone/neighborzone:

Create, read, update or delete the client zone.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials. **AutomaticallyRespondToH323Searches:** Determines what happens when the Expressway receives an H.323 search, destined for this zone. Off: an LRQ message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **AutomaticallyRespondToSIPSearches:** Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Off: a SIP OPTIONS message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **CallSignalingRoutedMode:** Specifies how the Expressway handles the signaling for calls to and from this neighbor. Auto: signaling is taken as determined by the Call routed mode configuration. Always: signaling is always taken for calls to or from this neighbor, regardless of the Call routed mode configuration. Default: Auto. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway. It will be used for H323 calls to and from the traversal client. **HopCount:** Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15.	Reads the zone data.

Method	Request Body	Response Code	Response Body	Comment
			InterworkingSIPSearchStrategy: Determines how the Expressway searches for SIP endpoints when interworking an H.323 call. Default: Options. **MonitorPeerStatus:** Specifies whether the Expressway monitors the status of the zones peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive. Default: Yes. **Name:** Name of the zone. **PeerAddress:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es , this is the FQDN of one of the peers in that cluster. **SIPAuthenticationTrustMode:** Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within theExpressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials. Default: Off. **SIPEncryptionMode:** Determines whether or not the Expressway allows encrypted SIP calls on this zone. Auto: SIP calls are encrypted if a secure SIP transport (TLS) is used. Microsoft: SIP calls are encrypted using MS-SRTP. Off: SIP calls are never encrypted. Default: Auto. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted. Default: Auto.	

Method	Request Body	Response Code	Response Body	Comment
			SIPMediaICESupport: Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultipartMIMEStripMode:** Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservation:** Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone will be poisoned such that if they are received by the local Expressway again they will be rejected. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPProxyRequireHeaderStripList:** A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified. **SIPREFERMode:** Determines how SIP REFER requests are handled. Forward: SIP REFER requests are forwarded to the target. Terminate: SIP REFER requests are terminated by the Expressway. Default: Forward.	

Method	Request Body	Response Code	Response Body	Comment
			SIPRecordRouteAddressType: Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, aTLS verify subject name must be specified. Default: Off. **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **SIPUDPBFCPFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/BFCP This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUDPIXFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUPDATEStripMode:** Determines whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone. Default: Off. **SendEmptyINVITEForInterworkedCalls:** Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. On: SIP INVITEs with no SDP are generated and sent to this neighbor. Off: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor. **Status:** The status of the zone. **ZoneProfile:** Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Default: Default. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials. **AutomaticallyRespondToH323Searches:** Determines what happens when the Expressway receives an H.323 search, destined for this zone. Off: an LRQ message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **AutomaticallyRespondToSIPSearches:** Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Off: a SIP OPTIONS message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **CallSignalingRoutedMode:** Specifies how the Expressway handles the signaling for calls to and from this neighbor. Auto: signaling is taken as determined by the Call routed mode configuration. Always: signaling is always taken for calls to or from this neighbor, regardless of the Call routed mode configuration. Default: Auto. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway. It will be used for H323 calls to and from the traversal client. **HopCount:** Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15.	201	{ **Message:** Success / Failure/ Info message for the operation. }	Creates neighbor zone.

Method	Request Body	Response Code	Response Body	Comment
	InterworkingSIPSearchStrategy: Determines how the Expressway searches for SIP endpoints when interworking an H.323 call. Default: Options. **MonitorPeerStatus:** Specifies whether the Expressway monitors the status of the zones peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive. Default: Yes. **Name:** Name of the zone. Range 1 to 50 characters. **PeerAddress:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es , this is the FQDN of one of the peers in that cluster. **SIPAuthenticationTrustMode:** Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within theExpressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials. Default: Off. **SIPEncryptionMode:** Determines whether or not the Expressway allows encrypted SIP calls on this zone. Auto: SIP calls are encrypted if a secure SIP transport (TLS) is used. Microsoft: SIP calls are encrypted using MS-SRTP. Off: SIP calls are never encrypted. Default: Auto. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted. Default: Auto.			

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaICESupport: Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultipartMIMEStripMode:** Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservation:** Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone will be poisoned such that if they are received by the local Expressway again they will be rejected. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPProxyRequireHeaderStripList:** A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified. **SIPREFERMode:** Determines how SIP REFER requests are handled. Forward: SIP REFER requests are forwarded to the target. Terminate: SIP REFER requests are terminated by the Expressway. Default: Forward. **SIPRecordRouteAddressType:** Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.			

Method	Request Body	Response Code	Response Body	Comment
	SIPTLSVerifyMode: Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, aTLS verify subject name must be specified. Default: Off. **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **SIPUDPBFCPFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/BFCP This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUDPIXFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUPDATEStripMode:** Determines whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone. Default: Off. **SendEmptyINVITEForInterworkedCalls:** Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. On: SIP INVITEs with no SDP are generated and sent to this neighbor. Off: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor. **ZoneProfile:** Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Default: Default. } ***Required:*** *Name, PeerAddress.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials. **AutomaticallyRespondToH323Searches:** Determines what happens when the Expressway receives an H.323 search, destined for this zone. Off: an LRQ message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **AutomaticallyRespondToSIPSearches:** Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Off: a SIP OPTIONS message is sent to the zone. On: searches are responded to automatically, without being forwarded to the zone. Default: Off. **CallSignalingRoutedMode:** Specifies how the Expressway handles the signaling for calls to and from this neighbor. Auto: signaling is taken as determined by the Call routed mode configuration. Always: signaling is always taken for calls to or from this neighbor, regardless of the Call routed mode configuration. Default: Auto. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway. It will be used for H323 calls to and from the traversal client. **HopCount:** Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15.	200	{ **Message:** Success/Failure/ Info message for the operation. }	Update zone configuration

Method	Request Body	Response Code	Response Body	Comment
	InterworkingSIPSearchStrategy: Determines how the Expressway searches for SIP endpoints when interworking an H.323 call. Default: Options. **MonitorPeerStatus:** Specifies whether the Expressway monitors the status of the zones peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive. Default: Yes. **Name:** Name of the zone. Range 1 to 50 characters. **NewName:** New name of the zone. Range 1 to 50 characters. **PeerAddress:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es , this is the FQDN of one of the peers in that cluster. **SIPAuthenticationTrustMode:** Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within theExpressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials. Default: Off. **SIPEncryptionMode:** Determines whether or not the Expressway allows encrypted SIP calls on this zone. Auto: SIP calls are encrypted if a secure SIP transport (TLS) is used. Microsoft: SIP calls are encrypted using MS-SRTP. Off: SIP calls are never encrypted. Default: Auto. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted. Default: Auto.			

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaICESupport: Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultipartMIMEStripMode:** Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservation:** Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone will be poisoned such that if they are received by the local Expressway again they will be rejected. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPProxyRequireHeaderStripList:** A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified. **SIPREFERMode:** Determines how SIP REFER requests are handled. Forward: SIP REFER requests are forwarded to the target. Terminate: SIP REFER requests are terminated by the Expressway. Default: Forward. **SIPRecordRouteAddressType:** Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.			

Method	Request Body	Response Code	Response Body	Comment
	SIPTLSVerifyMode: Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, aTLS verify subject name must be specified. Default: Off. **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **SIPUDPBFCPFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/BFCP This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUDPIXFilterMode:** Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. Off: INVITE requests are not modified. Default: Off. **SIPUPDATEStripMode:** Determines whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone. Default: Off. **SendEmptyINVITEForInterworkedCalls:** Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. On: SIP INVITEs with no SDP are generated and sent to this neighbor. Off: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor. **ZoneProfile:** Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Default: Default. } ***Required:*** *Name, PeerAddress.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** Name of the zone to be deleted. Range 1 to 50 characters. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete the zone.

/configuration/allowlist/autopaths:

Moebius API endpoint for HTTPAllowListAuto resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **path:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **ports:** Ports for which this HTTP allow rule is applied. **protocol:** Protocol for which this HTTP allow rule is applied. **servertype:** The type of server for this HTTP allow rule. **uuid:** Unique identifier for record. }	HTTP Get endpoint logic to retrieve auto generated HTTP allow list.

/configuration/allowlist/control:

Moebius API Endpoint for HTTPAllowListControl resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **methods:** **pattern:** }	This is a single record endpoint. Perform a HTTP GET against this resource

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **methods:** **pattern:** }	200	{ **Message:** Success/Failure/Info message for the operation. }	Update the singleton control record data. It will already be matched against a valid regular expression for this field at this point.

/configuration/allowlist/manualpaths:

API endpoint for creating, reading, updating or deleting the HTTP allow list records

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **url:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **pattern:** **uuid:** Unique identifier for record. }	Read all manually created HTTP allow list rules and modify them so they are consistent.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **url:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **uuid:** Unique identifier for record. }	200	None	Create a new manual HTTP allow list rule.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods.methods. **pattern:** **url:** URL to allow Mobile and Remote Access clients access to outside of enterprise network. **pattern:** **uuid:** Unique identifier for record. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Update record. Must provide the uuid and all fields needing to be updated

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **path:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **pattern:** **uuid:** Unique identifier for record. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete record.

/domaincerts/domain:

Get the list of defined multidomain certificate domains.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Message:** Success/Failure/Info message for the operations. **domains:** List of multidomain cert domains. **items:** One domain in a list of multidomain cert domains. }	Read the list of defined multidomain cert domains.

/domaincerts/domain/<domain>

Create, read, and delete a multidomain certificate domain. Note that read is only an existence check; no domain-specific data is returned, only the HTTP status code (OK or Not Found).

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Message:** Success/Failure/Info message for the operations. }	

Method	Request Body	Response Code	Response Body	Comment
POST	None	200	{ **Message:** Success/ Failure/ Info message for the operations. }	

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/ Failure/ Info message for the operations. }	

/domaincerts/domain/<domain>/cert:

Create, read, and delete a domain's certificate information. There is no separate update operation, create is also used to update.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Message:** Success/Failure/Info message for the operations. **cert-pem:** JSON-encoded certificate PEM. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **cert-pem:** JSON-encoded certificate PEM. **key-pem:** JSON-encoded private key PEM. } **Required:** cert-pem	200	{ **Message:** Success/ Failure/ Info message for the operations. }	

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/ Failure/ Info message for the operations. }	

/domaincerts/domain/<domain>/csr:

Create, read, and delete a certificate signing request for a domain. Update operation is not allowed for CSRs.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Message:** Success/Failure/Info message for the operations. **cert-pem:** JSON-encoded certificate PEM. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **CommonName:** The common name field in the subject of the signing request. **Country:** The two-letter ISO code for the country where your organization is located. **DigestAlgorithm:** The Digest algorithm used for the signature. Default: sha256. **Email:** The email address to include in the certificate. **KeyLength:** The number of bits used for public and private key encryption. Default: 4096. **Locality:** The town or city where your organization is located. **Organization:** The name of the organization or business. **OrganizationalUnit:** The department name or organizational unit handling the certificate. **Province:** The province, region, county, or state where your organization is located. **SubjectAlternativeNames:** Additional SAN hostnames included in the signing request. **Required:** Country, Province, Locality, Organization, OrganizationalUnit.	200	{ **Message:** Success/ Failure/ Info message for the operations. }	

Method	Request Body	Response Code	Response Body	Comment
DELETE	None	200	{ **Message:** Success/ Failure/ Info message for the operations. }	

Cisco Expressway-C

/controller/server/cucm:

Update or read the Cisco Unified Communications Manager configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AxlUsername:** The username used by the Expressway to access the Unified CM publisher. The user must have the Standard AXL API Access role. Range: 1 to 1024 characters. **Publisher:** The FQDN or IP address of the Unified CM node. Range: 1 to 1024 characters. **TlsVerify:** State of the TLS verify mode. If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority. }	Read the available configuration.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AxlPassword:** The AXL password of the Unified CM. Range: 1 to 1024 characters. **AxlUsername:** The username used by the Expressway to access the Unified CM publisher. The user must have the Standard AXL API Access role. Range: 1 to 1024 characters. **Publisher:** The FQDN or IP address of the Unified CM node. Range 1 to 1024 characters. **TlsVerify:** State of the TLS verify mode. If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority. } ***Required:*** *Publisher, AxlUsername, AxlPassword.*	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Create a new configuration.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Publisher:** The FQDN or IP address of the Unified CM node. Range 1 to 1024 characters. } ***Required:*** *Publisher.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Deleting the Unified CM configuration.

/controller/server/imp:

Update or read the Cisco Unified Communications Manager IM and Presence Service configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AxlUsername:** The username used by the Expressway to access the Cisco Unified Communications Manager IM and Presence Service publisher. The user must have the Standard AXL API Access role. Range: 1 to 255 characters. **Publisher:** The FQDN or IP address of the Cisco Unified Communications Manager IM and Presence Service database publisher node. Range: 1 to 1024 characters. **TlsVerify:** State of the TLS verify mode. If TLS verify mode is enabled, the Cisco Unified Communications Manager IM and Presence Service node's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority. Default: On. }	Reads the available configuration.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AxlPassword:** The password used by the Expressway to access the Cisco Unified Communications Manager IM and Presence Service publisher. Range: 1 to 1024 characters. **AxlUsername:** The username used by the Expressway to access the Cisco Unified Communications Manager IM and Presence Service publisher. The user must have the Standard AXL API Access role. Range: 1 to 255 characters. **Publisher:** The FQDN or IP address of the Cisco Unified Communications Manager IM and Presence Service database publisher node. Range: 1 to 1024 characters. **TlsVerify:** State of the TLS verify mode. If TLS verify mode is enabled, the Cisco Unified Communications Manager IM and Presence Service node's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority. Default: On. } ***Required:*** *Publisher, AxlUsername, AxlPassword.*	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Create a new configuration.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Publisher:** The FQDN or IP address of the Cisco Unified Communications Manager IM and Presence Service database publisher node to be deleted. Range: 1 to 1024 characters. } ***Required:*** *Publisher.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete the Cisco Unified Communications Manager IM and Presence Service configuration.

/controller/zone/traversalclient:

Create, read, update or delete the traversal client configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway. It will be used for H323 calls to and from the traversal client. **H323Protocol:** Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. It will be used for H323 calls to and from the traversal client. Default: Assent. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range 1 to 50. **Peer Address:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es, this is the FQDN of one of the peers in that cluster.	

Method	Request Body	Response Code	Response Body	Comment
			RetryInterval: The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120. Range: 1 to 65534. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. On preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off.	

Method	Request Body	Response Code	Response Body	Comment
			SIPPort: The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534 Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **Status:** The status of the zone. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway. It will be used for H323 calls to and from the traversal client. **H323Protocol:** Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. It will be used for H323 calls to and from the traversal client. Default: Assent.	201	{ **Message:** Success/ Failure/ Info message for the operations. }	Creates Unified Communications traversal client.

Method	Request Body	Response Code	Response Body	Comment
	HopCount: Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. **Peer Address:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es, this is the FQDN of one of the peers in that cluster. **RetryInterval:** The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120. Range: 1 to 65534. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On.			

Method	Request Body	Response Code	Response Body	Comment
	SIPParameterPreservationMode: Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. On preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: off **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534 Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **Status:** The status of the zone. } ***Required:*** *Name, AuthenticationUserName, AuthenticationPassword, PeerAddress.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway. It will be used for H323 calls to and from the traversal client. **H323Protocol:** Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. It will be used for H323 calls to and from the traversal client. Default: Assent. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. **NewName:** The new name to the zone. Range: 0 to 50 characters.	200	{ **Message:** Success/ Failure/ Info message for the operations. }	Creates Unified Communications traversal client.

Method	Request Body	Response Code	Response Body	Comment
	Peer Address: Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es, this is the FQDN of one of the peers in that cluster. **RetryInterval:** The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120. Range: 1 to 65534. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On.			

Method	Request Body	Response Code	Response Body	Comment
	SIPParameterPreservationMode: Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. On preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: off **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534 Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** Name of the zone to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/ Failure/ Info message for the operation. }	Delete the zone.

/controller/zone/unifiedcommunicationstraversal:

Create, read, update or delete the unified communications traversal client zone.

Method	Request Body	Response Code	Response Body	Comment
GET	None		{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 0 to 50 characters. **Peer Address:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es, this is the FQDN of one of the peers in that cluster. **RetryInterval:** The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120. Range: 1 to 65534. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the device in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.	Reads the zone data.

Method	Request Body	Response Code	Response Body	Comment
			SIPMultistreamMode: Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. On: Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off: Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **Status:** The status of the zone. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 0 to 50 characters. **Peer Address:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es, this is the FQDN of one of the peers in that cluster. **RetryInterval:** The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120. Range: 1 to 65534.	201	{ **Message:** Success /Failure/ Info message for the operations. }	Creates Unified Communications traversal client.

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaICESupport: Controls how the Expressway supports ICE messages to and from the device in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. On: Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off: Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. } ***Required:*** *Name, AuthenticationUserName, AuthenticationPassword, PeerAddress.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 0 to 50 characters. **NewName:** The new name of zone. **Peer Address:** Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Cisco Expressway-Es, this is the FQDN of one of the peers in that cluster. **RetryInterval:** The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120. Range: 1 to 65534.		{ **Message:** Success/ Failure/ Info message for the operations. }	Updates the Unified CM traversal client zone configuration.

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaICESupport: Controls how the Expressway supports ICE messages to and from the device in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. On: Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off: Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** Name of the zone to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/Failure/Info message for the operations. }	Delete the unified communication traversal client zone.

Cisco Expressway-E

/edge/traversal/turn:

CRUD operations for TURN Rest API.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AuthenticationRealm:** The realm sent by the server in its authentication challenges. Default: TANDBERG. Range 1 to 255. **DelegatedCredentialChecking:** Controls whether the credential checking of TURN server requests is delegated. Default: Off. **MediaPortRangeEnd:** The upper port in the range used for TURN relays. Default: 29999. Range: 1024 to 65534. **MediaPortRangeStart:** The lower port in the range used for TURN relays. Default: 2400. Range: 1024 to 65534. **ServerStatus:** status of listening address. NumberOfActiveTurnClients: status of active turn clients. **NumberOfActiveTurnRelaysViaTCP:** status of active turn relays connected via TCP. **NumberOfActiveTurnRelaysViaUDP:** status of active turn relays connected via UDP. **Status:** status of TURN. **TURNRegPort:** The listening port for TURN requests. Restart the TURN services if you change this value. Default: 3479. Range: 1024 to 65534. **TurnReqPortRangeEnd:** The listening port for TURN requests. Restart the TURN services if you change this value. Default: 3483. Range: 1024 to 65534. **TurnReqPortRangeStart:** The listening port for TURN requests. Restart the TURN services if you change this value. Default: 3478. Range: 1024 to 65534. **TurnServices:** Determines whether the Expressway offers TURN services to traversal clients. Default: Off. **Required:** TurnServices, AuthenticationRealm, MediaPortRangeStart, MediaPortRangeEnd. }	Get the TURN configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AuthenticationRealm:** The realm sent by the server in its authentication challenges. Default: TANDBERG. Range 1 to 255. **DelegatedCredentialChecking:** Controls whether the credential checking of TURN server requests is delegated. Default: Off. **MediaPortRangeEnd:** The upper port in the range used for TURN relays. Default: 29999. Range: 1024 to 65534. **MediaPortRangeStart:** The lower port in the range used for TURN relays. Default: 2400. Range: 1024 to 65534. **TURNRegPort:** The listening port for TURN requests. Restart the TURN services if you change this value. Default: 3479. Range: 1024 to 65534. **TurnReqPortRangeEnd:** The listening port for TURN requests. Restart the TURN services if you change this value. Default: 3483. Maximum: 65534. Minimum: 1024. **TurnReqPortRangeStart:** The listening port for TURN requests. Restart the TURN services if you change this value. Default: 3478. Range: 1024 to 65534. **TurnServices:** Determines whether the Expressway offers TURN services to traversal clients. Default: Off. **Required:** TurnServices, AuthenticationRealm, MediaPortRangeStart, MediaPortRangeEnd. }	200	{ **Message:** Success/ Failure/ Info message for the operations. }	Update the TURN configuration.

/edge/xmpp:

Read or update the XMPP configuration.

Method	Request Body	Response Code	Response Body	Comment
GET	None.	200	{ **PrivacyMode:** Controls whether restrictions are applied to the set of federated domains. Default: Allow list. **RequireClientSideSecurityCerts:** Controls whether the certificate presented by the client is verified against Expressway's current trusted CA list and the revocation list if loaded. **SecurityMode:** Indicates if a TLS connection to servers is required, preferred, or not required. Default: TLS required. **UseStaticRoutes:** Indicates whether a controlled list of static routes, rather than DNS lookup, are used to locate federation XMPP addresses. Default: Off. **XmppFederationSupport:** Enable or disable support for XMPP federation. } ***Required:*** *XmppFederationSupport.*	Read the XMPP configuration.

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **DialBackSecret:** The dialback secret used for identity verification with federated XMPP servers. Range 1 to 1024. **PrivacyMode:** Controls whether restrictions are applied to the set of federated domains. Default: Allow list. **RequireClientSideSecurityCerts:** Controls whether the certificate presented by the client is verified against Expressway's current trusted CA list and the revocation list if loaded. **SecurityMode:** Indicates if a TLS connection to servers is required, preferred, or not required. Default: TLS required. **UseStaticRoutes:** Indicates whether a controlled list of static routes, rather than DNS lookup, are used to locate federation XMPP addresses. Default: Off. **XmppFederationSupport:** Enable or disable support for XMPP federation. } ***Required:*** *XmppFederationSupport.*	200	{ **Message:** Success/ Failure/Info message for the operation. }	Update the XMPP configuration.

/edge/zone/traversalserver:

Create, read, update or delete the traversal server zone.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **H323H46019DemultiplexingMode:** Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway will be used for H.323 calls to and from the traversal client. **H323Protocol:** Determines which of the two firewall traversal protocols will be used for H.323 calls to and from the traversal client. Default: Assent. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255.	Gets the zone configuration details for traversal server zone.

Method	Request Body	Response Code	Response Body	Comment
			Name: Name of the zone. Range: 1 to 50 characters. **SIPMediaEncryptionMode:** Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the device in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. On: Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off: Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off.	

Method	Request Body	Response Code	Response Body	Comment
			SIPTLSVerifySubjectName: The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **Status:** The status of the zone. **TCPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. **TCPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5. **TCPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2. **UDPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. **UDPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default:5. **UDPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **H323H46019DemultiplexingMode:** Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway will be used for H.323 calls to and from the traversal client. **H323Protocol:** Determines which of the two firewall traversal protocols will be used for H.323 calls to and from the traversal client. Default: Assent. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 1 to 50 characters.	201	{ **Message:** Success/Failure/ Info message for the operations. }	Creates traversal server zone and sets its parameters.

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaEncryptionMode: Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the device in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. On: Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off: Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off.			

Method	Request Body	Response Code	Response Body	Comment
	SIPTLSVerifySubjectName: The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **Status:** The status of the zone. **TCPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. **TCPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5. **TCPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2. **UDPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. **UDPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default:5. **UDPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2. } ***Required:*** *Name, AuthenticationUserName.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **H323H46019DemultiplexingMode:** Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off. **H323Mode:** Determines whether H.323 calls will be allowed to and from this zone. Default: Off. **H323Port:** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Cisco Expressway-E, this must be the port number that has been configured on the Cisco Expressway-E's Traversal Server zone associated with this Expressway will be used for H.323 calls to and from the traversal client. **H323Protocol:** Determines which of the two firewall traversal protocols will be used for H.323 calls to and from the traversal client. Default: Assent. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note if the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 1 to 50 characters. **NewName:** The new name of zone. Range: 1 to 50 characters.	200	{ **Message:** Success/Failure/ Info message for the operations. }	Updates zone configuration for Traversal Server.

Method	Request Body	Response Code	Response Body	Comment
	SIPMediaEncryptionMode: Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the device in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMode:** Determines whether SIP calls will be allowed to and from this zone. Default: Off. **SIPMultistreamMode:** Controls if the Expressway allows Multistream to and from devices in this zone. On: allow Multistream. Off: disallow Multistream. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. On: Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. Off: Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: Off. **SIPPoisonMode:** Determines if SIP requests sent to this zone are "poisoned" and, if received by the local Expressway again, then rejected. On: SIP requests sent out via this zone that are received again by this Expressway will be rejected. Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal. Default: Off. **SIPPort:** The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifyMode:** Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off.			

Method	Request Body	Response Code	Response Body	Comment
	SIPTLSVerifySubjectName: The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). **SIPTransport:** The transport protocol to use for SIP calls to and from the traversal client. Default: TLS. **Status:** The status of the zone. **TCPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. **TCPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5. **TCPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2. **UDPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. **UDPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default:5. **UDPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** Name of the zone to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/Failure/ Info message for the operations. }	Delete the traversal server zone.

/edge/zone/unifiedcommunicationstraversal:

Create, read, update or delete the unified communications traversal server.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note: If the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 1 to 50 characters. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMultistreamMode:** Controls if the Expresswayallows Multistream to and from devices in this zone. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. Default: Off. **SIPPoisonMode:** Determines whether SIP requests sent out to this zone are "poisoned" and, if received by the local Expressway again, then rejected. Default: Off.	Reads the zone data.

Method	Request Body	Response Code	Response Body	Comment
			SIPPort: The port on this Expressway to use for SIP firewall traversal to and from the traversal client. Note: This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061). Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifySubjectName:** The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). Range 1 to 128. **Status:** Status of the zone. **TCPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. Range: 1 to 65534. **TCPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5. Range: 1 to 65534. **TCPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2. Range: 1 to 65534. **UDPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. Range: 1 to 65534. **UDPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5. Range: 1 to 65534. **UDPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2. Range: 1 to 65534. }	

Method	Request Body	Response Code	Response Body	Comment
POST	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note: If the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 1 to 50 characters. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMultistreamMode:** Controls if the Expresswayallows Multistream to and from devices in this zone. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. Default: Off.	201	{ **Message:** Success/ Failure/Info message for the operations. }	Creates unified communications traversal server.

Method	Request Body	Response Code	Response Body	Comment
	SIPPoisonMode: Determines whether SIP requests sent out to this zone are "poisoned" and, if received by the local Expressway again, then rejected. Default: Off. **SIPPort:** The port on this Expressway to use for SIP firewall traversal to and from the traversal client. Note: This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061). Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifySubjectName:** The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). Range 1 to 128. **Status:** Status of the zone. **TCPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. Range: 1 to 65534. **TCPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5. Range: 1 to 65534. **TCPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2. Range: 1 to 65534. **UDPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. Range: 1 to 65534. **UDPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5. Range: 1 to 65534. **UDPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2. Range: 1 to 65534. } ***Required:*** *Name, AuthenticationUserName, SIPTLSVerifySubjectName.*			

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **AcceptProxiedRegistrations:** Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. **AuthenticationMode:** Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain, and SIP messages that originate from non-local domains. Default: Do not check credentials. **AuthenticationUserName:** The username used by the Expressway when connecting to the traversal server. Range: 1 to 1024 characters. **HopCount:** Specifies the hop count used when sending an alias search request to this zone. Note: If the search request comes from another zone, and already has a hop count assigned, the lower of the two values is used. Default: 15. Range: 1 to 255. **Name:** Name of the zone. Range: 1 to 50 characters. **SIPMediaICESupport:** Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off. **SIPMultistreamMode:** Controls if the Expresswayallows Multistream to and from devices in this zone. Default: On. **SIPParameterPreservationMode:** Determines whether the B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone. Default: Off.	200	{ **Message:** Success/ Failure/Info message for the operations. }	Updates zone configuration.

Method	Request Body	Response Code	Response Body	Comment
	SIPPoisonMode: Determines whether SIP requests sent out to this zone are "poisoned" and, if received by the local Expressway again, then rejected. Default: Off. **SIPPort:** The port on this Expressway to use for SIP firewall traversal to and from the traversal client. Note: This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061). Default: 7001. Range: 1024 to 65534. **SIPPreloadedSipRoutesSupport:** Enable this zone to to process or reject SIP INVITE requests that contain Route header. Default: Off. **SIPTLSVerifySubjectName:** The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). Range 1 to 128. **Status:** Status of the zone. **TCPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. Range: 1 to 65534. **TCPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5. Range: 1 to 65534. **TCPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2. Range: 1 to 65534. **UDPProbeKeepAliveInterval:** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewalls NAT bindings open. Default: 20. Range: 1 to 65534. **UDPProbeRetryCount:** Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5. Range: 1 to 65534. **UDPProbeRetryInterval:** Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2. Range: 1 to 65534. } ***Required:*** *Name.*			

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **Name:** Name of the zone to be deleted. } ***Required:*** *Name.*	200	{ **Message:** Success/ Failure/Info message for the operations. }	Delete the Unified CM traversal server zone. .

/configuration/allowlist/control:

Moebius API Endpoint for HTTPAllowListControl resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **methods:** **pattern:** }	This is a single record endpoint. Perform a HTTP GET against this resource

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **methods:** **pattern:** }	200	{ **Message:** Success/Failure/Info message for the operation. }	Update the singleton control record data. It will already be matched against a valid regular expression for this field at this point.

/configuration/allowlist/autopaths:

Moebius API endpoint for HTTPAllowListAuto resource.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **path:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **ports:** Ports for which this HTTP allow rule is applied. **protocol:** Protocol for which this HTTP allow rule is applied. **servertype:** The type of server for this HTTP allow rule. **uuid:** Unique identifier for record. }	HTTP Get endpoint logic to retrieve auto generated HTTP allow list.

/configuration/allowlist/manualpaths:

API endpoint for creating, reading, updating or deleting the HTTP allow list records

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **url:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **pattern:** **uuid:** Unique identifier for record. }	Read all manually created HTTP allow list rules and modify them so they are consistent.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **url:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **uuid:** Unique identifier for record. }	200	None	Create a new manual HTTP allow list rule.

/configuration/allowlist/manualpaths:

Method	Request Body	Response Code	Response Body	Comment
PUT	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods.methods. **pattern:** **url:** URL to allow Mobile and Remote Access clients access to outside of enterprise network. **pattern:** **uuid:** Unique identifier for record. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Update record. Must provide the uuid and all fields needing to be updated

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **description:** A meaningful description for this rule, to help you recognize its purpose. **methods:** Comma-separated list of the HTTP methods allowed by this rule. An empty string will configure default methods. **pattern:** **path:** The URL path to allow Mobile and Remote Access clients to access the URL from outside of the enterprise network. **pattern:** **uuid:** Unique identifier for record. }	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete record.

/optionkey:

Read, update or delete option keys.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **OptionKey:** The value of the key. **Status:** Current status of the key. } ***Required:*** *OptionKey.*	Read the option key available.

Method	Request Body	Response Code	Response Body	Comment
POST	{ **OptionKey:** The value of the key. } ***Required:*** *OptionKey.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Add an option key.

Method	Request Body	Response Code	Response Body	Comment
DELETE	{ **OptionKey:** The value of the option key. } ***Required:*** *OptionKey.*	200	{ **Message:** Success/Failure/Info message for the operation. }	Delete an option key.

/restart:

Perform a system restart.

Method	Request Body	Response Code	Response Body	Comment
POST	None	200	{ **Message:** Success/Failure/Info message for the operation. }	System restarts.

/sysinfo:

Get the system information.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ **Product Mode:** Mode is either Cisco Telepresence Video Communication Server Control/ Cisco Telepresence Video Communication Server Expressway/Expressway-C/Expressway-E **Restapi Version:** RestApi Component version **Software Version:** The software version. }	Provides software version, REST API version, product mode.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark