Cisco Expressway REST API

Reference Guide

First Published: June 2016

X8.8

Cisco Systems, Inc. www.cisco.com

Contents

Preface

Change History

Table 1 Reference Guide Change History

Date	Change	Reason
June 2016	Initial release.	

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`).

Common Between Cisco Expressway-C and Cisco Expressway-E

/common/certs/root:

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 message for the operation.
			}
				Write the root certificate to the default path. Request body contains the root CA data.

/common/certs/generate_csr:

Generate or read the Certificate Signing Request (CSR).

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	CSR content.	Gets the generated CSR from its path and displays the same.

Method	Request Body	Response Code	Response Body	Comment

POST	{
	Additional_FQDNS: Additional freeform hostnames included in the certificate.
	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.
	Country: The two-letter ISO code for the country where your organization is located.
	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.
	}
		200	{
			Message: Success message for the operation.
			}
				Generates the CSR and stores it in its path.

/common/certs/server:

The signed 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 message for the operation.
			}
				Write the server certificate to the default path. The request body contains the server certificate data.

/common/defaultlinks:

Check or create the default links.

Method	Request Body	Response Code	Response Body	Comment

POST	None	200	{
			Message: Successful creation of DefaultLinks.
			Status: Status OK.
			}
				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/mra:

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

Method	Request Body	Response Code	Response Body	Comment

GET	None	200	{
			Shows if MRA is enabled or disabled. 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.
			}
				Read the MRA configuration.

Method	Request Body	Response Code	Response Body	Comment

PUT	{
	Enabled: Enable or disable MRA.
	}
		200	{
			Enabled: Enable or disable MRA.
			}
				Update or get the current MRA configuration.

Cisco Expressway-C

/controller/domain:

Push, Get or Put the domain configuration.

Method	Request Body	Response Code	Response Body	Comment

GET	None	200	{
			edgesip: Service status of EdgeSIP domain.
			edgexmpp: Service status of the XMPP domain.
			index: The index value of the domain. Range 1 to 200 characters.
			Name: The name of the domain. Range 1 to 1024 characters.
			xmppfederation: Service status of the Jabber domain.
			}
				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.
	}
		200	{
			Message: Success 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 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 message for the operations.
			}
				Update the domain.

/controller/server/cucm:

The resource class to add and update the Cisco Unified Communications Manager configuration. Also lists all the current configuration.

Method	Request Body	Response Code	Response Body	Comment

GET	The Fully Qualified Domain Name (FQDN) or IP address of the Unified CM node. Range: 1 to 1024 characters.	200	{
			axl_username: 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.
			tls_verify: 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	{
	axl_password: The AXL password of the Unified CM. Range: 1 to 1024 characters.
	axl_username: 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.
	tls_verify: 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.
	}
		200	{
			Message: The result of the operation.
			}
				Create a new configuration.

/controller/server/imp:

The resource class to add and update the Cisco Unified Communications Manager IM and Presence Service configuration. Also lists all the current configuration.

Method	Request Body	Response Code	Response Body	Comment

GET	The FQDN or IP address of the Cisco Unified Communications Manager IM and Presence Service database publisher node. Range: 1 to 1024 characters.	200	{
			axl_username: 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.
			tls_verify: 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	{
	axl_password: The password used by the Expressway to access the Cisco Unified Communications Manager IM and Presence Service publisher. Range: 1 to 1024 characters.
	axl_username: 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.
	tls_verify: 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.
	}
		200	{
			Message: The result of the operation.
			}
				Create a new configuration.

/controller/zones/unifiedcommunicationstraversal:

Read, create, or update the unified communications traversal client.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ 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. CollaborationEdge: H323Port: H323Protocol: 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: PreloadedSIPRoutesSupport: Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header. Default: Off. Registrations: Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. 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.	Reads the zone data.

Method	Request Body	Response Code	Response Body	Comment
			SIPMediaEncryptionMode: 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: 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. Status: ZoneIndex: ZoneType: SIPPort: Specifies the port on the traversal server to use for SIP firewall traversal calls from this Expressway. If the traversal server is an 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. Note: This must be different from the listening ports used for the incoming TCP, TLS, and UDP SIP calls (typically 5060 and 5061). Default: 7001. Range: 1024 to 65534. Addresses: 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 server's 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. }	

Cisco Expressway-C

Method	Request Body	Response Code	Response Body	Comment

POST	{
	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.
	AuthenticationPassword: The password used by the Expressway when connecting to the traversal server. The maximum plaintext length is 128 characters. The password is then encrypted.
	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.
	New_Name: Apply a new name to the zone. Range 0 to 50 characters.
	PreloadedSIPRoutesSupport: Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header. Default: Off.
	Registrations: Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.
		200	{
			Message: Success message for the operations.
			}
				Creates Unified Communications traversal client.

	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. 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: Specifies the port on the traversal server to use for SIP firewall traversal calls from this Expressway. If the traversal server is an 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. Note: This must be different from the listening ports used for the incoming TCP, TLS, and UDP SIP calls (typically 5060 and 5061). Default: 7001. Range: 1024 to 65534. Addresses: 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 server's 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

PUT	{
	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.
	AuthenticationPassword: The password used by the Expressway when connecting to the traversal server. The maximum plaintext length is 128 characters. The password is then encrypted.
	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.
	New_name: Apply a new name to the zone. Range: 0 to 50 characters.
	PreloadedSIPRoutesSupport: Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header. Default: Off.
	Registrations: Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.
		200	{
			Message: Success message for the operation.
			}
				Updates the zone configuration.

	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. 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: Specifies the port on the traversal server to use for SIP firewall traversal calls from this Expressway. If the traversal server is an 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. Note: This must be different from the listening ports used for the incoming TCP, TLS, and UDP SIP calls (typically 5060 and 5061). Default: 7001. Range: 1024 to 65534. Addresses: 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 server's 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. }			

Cisco Expressway-E

/edge/credential:

Push, Get or Put credentials on to the local database for authentication.

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 plaintext length is 128 characters, which will then be encrypted.
	}
		200	{
			Message: Success message for the operations.
			}
				Adds 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.
	New_Name: Change the existing credential name to another name. Range: 1 to 1024 characters.
	New_Password: Change password of the existing credential. The maximum plaintext length is 128 characters, which is then encrypted.
	}
		200	{
			Message: Success message for the operations.
			}
				Update either name, password or both for an existing credential.

/edge/zone/unifiedcommunicationstraversal:

Read, create, or update the unified communications traversal server.

Method	Request Body	Response Code	Response Body	Comment
GET	None	200	{ AuthenticationMode: Controls how 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: Name used by the traversal client when authenticating with the traversal server. If the traversal client is a Expressway, this must be the username configured for that Expressway's traversal client zone. For other types of traversal clients, refer to the online help for further information. Range 1 to 1024 characters. H323Port: H232Protocol: 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 1024 characters. Registrations: Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. SIPMediaEncryptionMode: 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. 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. SIPPreloadedSipRoutesAccept: Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off. SIPProtocol: SIPTLSVerifyMode: 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 attribute). Range: 1 to 1024 characters. SIPTransport: Status: 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. Zone Index: Zone Type: }	

Method	Request Body	Response Code	Response Body	Comment

POST	{
	AuthenticationMode: Controls how 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: Name used by the traversal client when authenticating with the traversal server. If the traversal client is a Expressway, this must be the username configured for that Expressway's traversal client zone. For other types of traversal clients, refer to the online help for further information. 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 1024 characters.
	New name: Apply a new name to the zone. Range: 1 to 1024 characters.
	Registrations: Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.
	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.
	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.
	SIPPort: Port to use for SIP firewall traversal to and from traversal client
	SIPPreloadedSipRoutesAccept: Enable this zone to process or reject SIP INVITE requests that contain Route header. Default: Off.
	SIPTLSVerifySubjectName: The certificate holder's name to
		200	{
			Message: Success message for the operations.
			}
				Creates unified communications traversal server.

Method	Request Body	Response Code	Response Body	Comment
	look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attribute). Range: 1 to 1024 characters. 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

PUT	{
	AuthenticationMode: Controls how 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: Name used by the traversal client when authenticating with the traversal server. If the traversal client is a Expressway, this must be the username configured for that Expressway's traversal client zone. For other types of traversal clients, refer to the online help for further information. 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 1024 characters.
	New_Name: Apply a new name to the zone. Range: 1 to 1024 characters.
	Registrations: Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.
	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.
	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.
	SIPPort: Port to use for SIP firewall traversal to and from traversal client.
	SIPPreloadedSipRoutesAccept: Enable this zone 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
		200	{
			Message: Success message for the operations.
			}
				Updates zone configuration.

Method	Request Body	Response Code	Response Body	Comment
	either the Subject Common Name or the Subject Alternative Name attribute). Range: 1 to 1024 characters. 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. }			

Option key

/optionkey:

The resource class to add, remove and get all option keys.

Method	Request Body	Response Code	Response Body	Comment

GET	{
	option_key: The value of the key.
	}
		200	{
			option_key: The value of the key.
			status: Current status of the key.
			}
				Read the option key available.

POST	{
	option_key: The value of the key.
	}
		200	{
			option_key: The value of the key.
			status: Current status of the key.
			}
				Add an option key.

Cisco Legal Information

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.

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