Device Authentication

This section provides information about the Expressway's authentication policy and the pages that appear under the **Configuration** > **Authentication** menu.

About Device Authentication

Device authentication is the verification of the credentials of an incoming request to the Expressway from a device or external system. It is used so that certain functionality may be reserved for known and trusted users.

Mobile and Remote Access devices

You do not have to make any explicit configuration on the Expressway regarding the authentication of devices that are registering to Unified CM via the Expressway. If the Expressway is the authenticating agent for these devices (compared to an external IdP), then it automatically handles the authentication of these devices against their home Unified CM clusters.

Rich media sessions

Devices communicating with the Expressway that are participating in rich media sessions are subject to the Expressway's configurable authentication policy.

When device authentication is enabled, any device that attempts to communicate with the Expressway is challenged to present its credentials (typically based on a username and password). The Expressway will then verify those credentials against its Configuring Authentication to Use the Local Database.

Expressway authentication policy can be configured separately for each zone. This means that both authenticated and unauthenticated devices could be allowed to communicate with the same Expressway if required. Subsequent call routing decisions can then be configured with different rules based upon whether a device is authenticated or not.

Authentication Policy

Authentication Policy Configuration Options

Authentication policy behavior varies for H.323 messages, SIP messages received from local domains and SIP messages from non-local domains.

The primary authentication policy configuration options and their associated behavior are as follows:

- **Check credentials:** Verify the credentials using the relevant authentication method.

  Note In some scenarios, messages are not challenged, see below.

- **Do not check credentials:** Do not verify the credentials and allow the message to be processed.
- **Treat as authenticated:** Do not verify the credentials and allow the message to be processed as if it is has been authenticated. This option can be used to cater for endpoints from third-party suppliers that do not support authentication within their registration mechanism.

  Note In some scenarios, messages are allowed but will still be treated as though they are unauthenticated, see below.

Authentication policy is selectively configurable for different zone types, based on whether they receive messaging:

- The Default Zone, Neighbor zones, traversal client zones, traversal server zones and Unified Communications traversal zones all allow configuration of authentication policy.
- DNS and ENUM zones do not receive messaging and so have no authentication policy configuration.

To edit a zone's **Authentication policy**, go to **Configuration** > **Zones** > **Zones** and click the name of the zone. The policy is set to *Do not check credentials* by default when you create a new zone.

The behavior varies for H.323 and SIP messages as shown in the tables below:

H.323

Policy	Behavior
Check credentials	Messages are classified as either authenticated or unauthenticated depending on whether any credentials in the message can be verified against the authentication database. If no credentials are supplied, the message is always classified as unauthenticated.
Do not check credentials	Message credentials are not checked and all messages are classified as unauthenticated.

Policy	Behavior
Treat as authenticated	Message credentials are not checked and all messages are classified as authenticated.

SIP

The behavior for SIP messages at the zone level depends upon the SIP Authentication Trust mode setting (meaning whether the Expressway trusts any pre-existing authenticated indicators - known as P-Asserted Identity headers - within the received message) and whether the message was received from a local domain (a domain for which the Expressway is authoritative) or a non-local domain.

Policy	Trust	In local domain	Outside local domain
Check credentials	Off	Messages are challenged for authentication. Messages that fail authentication are rejected. Messages that pass authentication are classified as authenticated and a P-Asserted-Identity header is inserted into the message.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.
	On	Messages with an existing P-Asserted-Identity header are classified as authenticated, without further challenge. The P-Asserted-Identity header is passed on unchanged (keeping the originator's asserted ID). Messages without an existing P-Asserted-Identity header are challenged. If authentication passes, the message is classified as authenticated and a P-Asserted-Identity header is inserted into the message. If authentication fails, the message is rejected.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.
Do not check credentials	Off	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.

Policy	Trust	In local domain	Outside local domain
	On	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.
Treat as authenticated	Off	Messages are not challenged for authentication. All messages are classified as authenticated. Any existing P-Asserted-Identity header is removed and a new one containing the Expressway's originator ID is inserted into the message.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.
	On	Messages are not challenged for authentication. All messages are classified as authenticated. Messages with an existing P-Asserted-Identity header are passed on unchanged. Messages without an existing P-Asserted-Identity header have one inserted.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.

Controlling System Behavior for Authenticated and Non-Authenticated Devices

How calls and other messaging from authenticated and non-authenticated devices are handled depends on how search rules, external policy services and CPL are configured.

Search rules

When configuring a search rule, use the **Request must be authenticated** attribute to specify whether the search rule applies only to authenticated search requests or to all requests.

External policy services

External policy services are typically used in deployments where policy decisions are managed through an external, centralized service rather than by configuring policy rules on the Expressway itself. You can configure the Expressway to use policy services in the following areas:

- Registration Policy

- Search rules (dial plan)
- Call Policy
- User Policy (FindMe)

When the Expressway uses a policy service it sends information about the call or registration request to the service in a POST message using a set of name-value pair parameters. Those parameters include information about whether the request has come from an authenticated source or not.

See *Cisco Expressway External Policy Deployment Guide* at the Cisco Expressway Series Configuration Guides page.

CPL

If you are using the Call Policy rules generator on the Expressway, source matches are carried out against authenticated sources. To specify a match against an unauthenticated source, just use a blank field. (If a source is not authenticated, its value cannot be trusted).

If you use uploaded, handcrafted local CPL to manage your Call Policy, you are recommended to make your CPL explicit as to whether it is looking at the authenticated or unauthenticated origin.

- If CPL is required to look at the unauthenticated origin (for example, when checking non-authenticated callers) the CPL must use `unauthenticated-origin`. (However, if the user is unauthenticated, they can call themselves whatever they like; this field does not verify the caller.)
- To check the authenticated origin (only available for authenticated or "treat as authenticated" devices) the CPL should use `authenticated-origin`.

Note Due to the complexity of writing CPL scripts, you are recommended to use an external policy service instead.

SIP Authentication Trust

If the Expressway is configured to use About Device Authentication it will authenticate incoming SIP INVITE requests. If the Expressway then forwards the request on to a neighbor zone such as another Expressway, that receiving system will also authenticate the request. In this scenario the message has to be authenticated at every hop.

To simplify this so that a device's credentials only have to be authenticated once (at the first hop), and to reduce the number of SIP messages in your network, you can configure neighbor zones to use the **Authentication trust mode** setting.

This is then used in conjunction with the zone's authentication policy to control whether pre-authenticated SIP messages received from that zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. Pre-authenticated SIP requests are identified by the presence of a P-Asserted-Identity field in the SIP message header as defined by RFC 3326.

The **Authentication trust mode** settings are:

- *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*.

Note

- We recommend that you enable authentication trust only if the neighbor zone is part of a network of trusted SIP servers.
- Authentication trust is automatically implied between traversal server and traversal client zones.

Device Provisioning and Authentication Policy

The Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the Expressway. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

The Expressway must be configured with appropriate device authentication settings, otherwise provisioning related messages will be rejected:

- Initial provisioning authentication (of a subscribe message) is controlled by the authentication policy setting on the Default Zone. (The Default Zone is used as the device is not yet registered.)
- The Default Zone and any traversal client zone's authentication policy must be set to either *Check credentials* or *Treat as authenticated*, otherwise provisioning requests will fail.

In each case, the Expressway performs its authentication checking against the local database. This includes all credentials supplied by Cisco TMS.

For more information about provisioning configuration in general, see Cisco TMS Provisioning Extension Deployment Guide.

Authentication Methods

Configuring Authentication to Use the Local Database

The local authentication database is included as part of your Expressway system and does not require any specific connectivity configuration. It is used to store user account authentication credentials. Each set of credentials consists of a **name** and **password**.

The credentials in the local database can be used for device (SIP), traversal client, and TURN client authentication.

Adding credentials to the local database

To enter a set of device credentials:

1. Go to **Configuration** > **Authentication** > **Devices** > **Local database** and click **New**.
2. Enter the **Name** and **Password** that represent the device's credentials.
3. Click **Create credential**.

Note The same credentials can be used by more than one device.

Credentials managed within Cisco TMS (for device provisioning)

When the Expressway is using TMS Provisioning Extension services, the credentials supplied by the Users service are stored in the local authentication database, along with any manually configured entries. The **Source** column identifies whether the user account name is provided by **TMS**, or is a **Local** entry. Only **Local** entries can be edited.

Incorporating Cisco TMS credentials within the local database means that Expressway can authenticate all messages (i.e. not just provisioning requests) against the same set of credentials used within Cisco TMS.

Local database authentication in combination with H.350 directory authentication

You can configure the Expressway to use both the local database and an H.350 directory.

If an H.350 directory is configured, the Expressway will always attempt to verify any Digest credentials presented to it by first checking against the local database before checking against the H.350 directory.

Local database authentication in combination with Active Directory (direct) authentication

If Active Directory (direct) authentication has been configured and NTLM protocol challenges is set to *Auto*, then NTLM authentication challenges are offered to those devices that support NTLM.

- NTLM challenges are offered in addition to the standard Digest challenge.
- Endpoints that support NTLM will respond to the NTLM challenge in preference to the Digest challenge, and the Expressway will attempt to authenticate that NTLM response.

Authenticating with External Systems

The **Outbound connection credentials** page (**Configuration** > **Authentication** > **Outbound connection credentials**) is used to configure a username and password that the Expressway will use whenever it is required to authenticate with external systems.

For example, when the Expressway is forwarding an invite from an endpoint to another Expressway, that other system may have authentication enabled and will therefore require your local Expressway to provide it with a username and password.

Note These settings are not used by traversal client zones. Traversal clients, which must always authenticate with traversal servers before they can connect, configure their connection credentials per traversal client zone.