Registration Control

About Registrations

For an endpoint to use the Expressway as its SIP registrar or H.323 gatekeeper, the endpoint must first register with the Expressway. The Expressway can be configured to control which devices are allowed to register with it by using the following mechanisms:

- A device authentication process based on the username and password supplied by the endpoint.
- A Configuring Registration Restriction Policy that uses either About Allow and Deny Lists or an external policy service to specify which aliases can and cannot register with the Expressway.
- Restrictions based on IP addresses and subnet ranges through the specification of subzone membership rules and subzone registration policies.

You can use these mechanisms together. For example, you can use authentication to verify an endpoint's identity from a corporate directory, and registration restriction to control which of those authenticated endpoints may register with a particular Expressway.

You can also control some protocol-specific behavior, including:

- The **Registration conflict mode** and **Auto discover** settings for H.323 registrations
- The **SIP registration proxy mode** for SIP registrations

For specific information about how registrations are managed across peers in a cluster, see the Sharing Registrations Across Peers section.

In a Unified Communications deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the Expressway provides secure firewall traversal and line-side support for Unified CM registrations. When configuring a domain, you can select whether Cisco Unified Communications Manager or Expressway provides registration and provisioning services for the domain.

Finding an Expressway with Which to Register

Before an endpoint can register with a Expressway, it must determine which Expressway it can or should be registering with. This setting is configured on the endpoint, and the process is different for SIP and H.323.

Note If you select MRA (for example), Expressway E will register devices even upon disabling the **Registration** tab.

MCU, Gateway, and Content Server Registration

H.323 systems such as gateways, MCUs and Content Servers can also register with a Expressway. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the Expressway when registering. The Expressway will then know to route all calls that begin with that prefix to the gateway, MCU or Content Server as appropriate. These prefixes can also be used to control registrations.

SIP devices cannot register prefixes. If your dial plan dictates that a SIP device should be reached via a particular prefix, then you should add the device as a neighbor zone with an associated search rule using a pattern match equal to the prefix to be used.

Configuring Registration Restriction Policy

The **Registration configuration** page (**Configuration** > **Registration** > **Configuration**) is used to control how the Expressway manages its registrations.

The **Restriction policy** option specifies the policy to use when determining which endpoints may register with the Expressway. The options are:

- *None*: Any endpoint may register.
- *Allow List*: Only those endpoints with an alias that matches an entry in the Allow List may register.
- *Deny List*: All endpoints may register, unless they match an entry on the Deny List.
- *Policy service*: Only endpoints that register with details allowed by the external policy service may register.

The default is *None*.

If you use an *Allow List* or *Deny List*, you must also go to the appropriate Configuring the Registration Allow List or Configuring the Registration Deny List configuration page to create the list.

The *Policy service* option is used if you want to refer all registration restriction policy decisions out to an external service. If you select this option an extra set of configuration fields appear so that you can specify the connection details of the external service. See Configuring Registration Policy to Use an External Service.

Registering Aliases

After the device authentication process (if required) has been completed, the endpoint will then attempt to register its aliases with the Expressway.

H.323

When registering, the H.323 endpoint presents the Expressway with one or more of the following:

- one or more H.323 IDs
- one or more E.164 aliases
- one or more URIs

Users of other registered endpoints can then call the endpoint by dialing any of these aliases.

- You are recommended to register your H.323 endpoints using a URI. This facilitates interworking between SIP and H.323, as SIP endpoints register using a URI as standard.
- You are recommended to not use aliases that reveal sensitive information. Due to the nature of H.323, call setup information is exchanged in an unencrypted form.

SIP

When registering, the SIP endpoint presents the Expressway with its contact address (IP address) and logical address (Address of Record). The logical address is considered to be its alias, and will generally be in the form of a URI.

H.350 directory authentication and registrations

If the Expressway is using an H.350 directory service to authenticate registration requests, the **Source of aliases for registration** setting is used to determine which aliases the endpoint is allowed to attempt to register with. See “Using an H.350 directory service lookup via LDAP” for more information.

Attempts to register using an existing alias

An endpoint may attempt to register with the Expressway using an alias that is already registered to the system. How this is managed depends on how the Expressway is configured and whether the endpoint is SIP or H.323.

- **H.323**: An H.323 endpoint may attempt to register with the Expressway using an alias that has already been registered on the Expressway from another IP address. You can control how the Expressway behaves in this situation by configuring the **Registration conflict mode** , on the H.323 page (**Configuration** > **Protocols** > **H.323**).
- **SIP**: A SIP endpoint will always be allowed to register using an alias that is already in use from another IP address. When a call is received for this alias, all endpoints registered using that alias will be called simultaneously. This SIP feature is known as “forking”.

Blocking registrations

If you have configured the Expressway to use a Configuring the Registration Deny List, you will have an option to block the registration. This will add all the aliases used by that endpoint to the Deny List.

Removing existing registrations

After a restriction policy has been activated, it controls all registration requests from that point forward. However, any existing registrations may remain in place, even if the new list would otherwise block them. Therefore, you are recommended to manually remove all existing unwanted registrations after you have implemented a restriction policy.

To manually remove a registration, go to **Status** > **Registrations** > **By device**, select the registrations you want to remove, and click **Unregister**.

If the registered device is in an active call and its registration is removed (or expires), the effect on the call is dependent on the protocol:

- **H.323**: The call is taken down.
- **SIP**: The call stays up by default. This SIP behavior can be changed but only via the CLI by using the command `xConfiguration SIP Registration Call Remove`.

Re-registrations

All endpoints must periodically re-register with the Expressway in order to keep their registration active. If you do not manually delete the registration, the registration could be removed when the endpoint attempts to re-register, but this depends on the protocol being used by the endpoint:

- H.323 endpoints may use "light" re-registrations which do not contain all the aliases presented in the initial registration, so the re-registration may not get filtered by the restriction policy. If this is the case, the registration will not expire at the end of the registration timeout period and must be removed manually.
- SIP re-registrations contain the same information as the initial registrations so will be filtered by the restriction policy. This means that, after the list has been activated, all SIP registrations will disappear at the end of their registration timeout period.

The frequency of re-registrations is determined by the **Registration controls** setting for SIP (**Configuration** > **Protocols** > **SIP**) and the **Time to live** setting for H.323 (**Configuration** > **Protocols** > **H.323**).

Note By reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.

About Allow and Deny Lists

When an endpoint attempts to register with the Expressway it presents a list of aliases. One of the methods provided by the Expressway to control which endpoints are allowed to register is to set the **Restriction policy** (on the Configuring Registration Restriction Policy page) to *Allow List* or *Deny List* and then to include any one of the endpoint's aliases on the Allow List or the Deny List as appropriate. Each list can contain up to 2,500 entries.

When an endpoint attempts to register, each of its aliases is compared with the patterns in the relevant list to see if it matches. Only one of the aliases needs to appear in the Allow List or the Deny List for the registration to be allowed or denied.

For example, if the **Restriction policy** is set to *Deny List* and an endpoint attempts to register using three aliases, one of which matches a pattern on the Deny List, that endpoint's registration will be denied. Likewise, if the **Restriction policy** is set to *Allow List*, only one of the endpoint's aliases needs to match a pattern on the Allow List for it to be allowed to register using all its aliases.

Allow Lists and Deny Lists are mutually exclusive: only one may be in use at any given time. You can also control registrations at the subzone level. Each subzone's registration policy can be configured to allow or deny registrations assigned to it via the subzone membership rules.

Configuring the Registration Allow List

The **Registration Allow List** page (**Configuration** > **Registration** > **Allow List**) shows the endpoint aliases and alias patterns that are allowed to register with the Expressway. Only one of an endpoint's aliases needs to match an entry in the Allow List for the registration to be allowed.

To use the Allow List, you must select a **Restriction policy** of *Allow List* on the Configuring Registration Restriction Policy page.

The configurable options are:

Field	Description	Usage tips
Description	An optional free-form description of the entry.	
Pattern type	The way in which the **Pattern string** must match the alias. Options are: *Exact*: The alias must match the pattern string exactly. *Prefix*: The alias must begin with the pattern string. *Suffix*: The alias must end with the pattern string. *Regex*: The pattern string is a regular expression.	You can test whether a pattern matches a particular alias by using the Check pattern tool (**Maintenance** > **Tools** > **Check pattern**).
Pattern string	The pattern against which an alias is compared.	

Configuring the Registration Deny List

The **Registration Deny List** page (**Configuration** > **Registration** > **Deny List**) shows the endpoint aliases and alias patterns that are not allowed to register with the Expressway. Only one of an endpoint's aliases needs to match an entry in the Deny List for the registration to be denied.

To use the Deny List, you must select a **Restriction policy** of *Deny List* on the Configuring Registration Restriction Policy page.

The configurable options are:

Field	Description	Usage tips
Description	An optional free-form description of the entry.	

Field	Description	Usage tips
Pattern type	The way in which the **Pattern string** must match the alias. Options are: *Exact*: The alias must match the pattern string exactly. *Prefix*: The alias must begin with the pattern string. *Suffix*: The alias must end with the pattern string. *Regex*: The pattern string is a regular expression.	You can test whether a pattern matches a particular alias by using the Check pattern tool (**Maintenance** > **Tools** > **Check pattern**).
Pattern string	The pattern against which an alias is compared.	

Configuring Registration Policy to Use an External Service

To configure Registration Policy to refer all registration restriction policy decisions out to an external service:

Step 1 Go to **Configuration** > **Registration** > **Configuration**.

Step 2 Select a **Restriction policy** of *Policy service*.

Step 3 Configure the fields as follows:

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service. The default is *HTTPS*.	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.
Certificate verification mode	When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. If *On*, for the Expressway to connect to a policy server over HTTPS, the Expressway must have a root CA certificate loaded that authorizes that server's server certificate. Also the certificate's Subject Common Name or Subject Alternative Name must match one of the **Server address** fields below.	The Expressway's root CA certificates are loaded via (**Maintenance** > **Security** > **Trusted CA certificate**).
HTTPS certificate revocation list (CRL) checking	Enable this option if you want to protect certificate checking using CRLs and you have manually loaded CRL files, or you have enabled automatic CRL updates.	Go to **Maintenance** > **Security** > **CRL management** to configure how the Expressway uploads CRL files.

Field	Description	Usage tips
Server address 1 - 3	Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending **:<port>** to the address.	If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved. For resiliency, up to three server addresses can be supplied.
Path	Enter the URL of the service on the server.	
Status path	The **Status path** identifies the path from where the Expressway can obtain the status of the remote service. The default is *status*.	The policy server must supply return status information, see Policy Server Status and Resiliency.
Username	The username used by the Expressway to log in and query the service.	
Password	The password used by the Expressway to log in and query the service.	The maximum plaintext length is 30 characters (which is subsequently encrypted).
Default CPL	This is the fallback CPL used by the Expressway if the service is not available.	You can change it, for example, to redirect to an answer service or recorded message. For more information, see Default CPL for Policy Services.

Step 4 Click **Save**.

The Expressway should connect to the policy service server and start using the service for Registration Policy decisions.

Any connection problems will be reported on this page. Check the **Status** area at the bottom of the page and check for additional information messages against the **Server address** fields.