User Accounts

About User Accounts

Expressway has two types of user account for normal operation:

- **Administrator accounts** - Used to configure the Expressway.
- **FindMe accounts** - Used by individuals in an enterprise to configure their FindMe profile. (FindMe account configuration via Expressway does not apply if the Expressway is using TMS Provisioning Extension services to provide FindMe data.)

Account Authentication

Administrator and FindMe accounts must be authenticated before access is allowed to the Expressway.

Expressway can authenticate accounts locally, or against a remote directory service using LDAP (currently, Windows Active Directory is supported), or using a combination of local and remotely managed accounts. The remote option allows administration groups to be set up in the directory service for all Expressways in an enterprise, removing the need to have separate accounts on each Expressway.

See Configuring Remote Account Authentication Using LDAP for more information about setting up remote authentication.

If a remote source is used for either administrator or FindMe account authentication, you also need to configure Expressway with the following:

- Appropriate LDAP server connection settings.

- Administrator groups and/or FindMe groups that match the corresponding group names already set up in the remote directory service to manage administrator and FindMe access to this Expressway (see Configuring Administrator Groups and Configuring user groups).

The Expressway can also be configured to use certificate-based authentication. This would typically be required if the Expressway is deployed in a highly-secure environment.

Password complexity

Complexity requirements can be specified for locally-managed passwords, from the Configuring Password Security page (**Users** > **Password security**).

All passwords and usernames are case sensitive.

Account Types

Administrator accounts

Administrator accounts are used to configure the Expressway.

The Expressway has a default **admin** local administrator account with full read-write access. It can be used to access the Expressway using the web interface, the API interface or the CLI.

Note You cannot access the Expressway via the default **admin** account if a *Remote only* authentication source is in use.

You can add additional local administrator accounts which can be used to access the Expressway, using the web and API interfaces only.

Remotely managed administrator accounts can also be used to access the Expressway, using the web interface, the API interface, or the CLI.

You can configure one administrator account to be the emergency account. This special account gives access to the Expressway even when it disallows local authentication, in case remote authentication is not possible.

Configuration log

The Configuration log records all login attempts and configuration changes made using the web interface, and can be used as an audit trail. This is particularly useful when you have multiple administrator accounts.

Multiple admin sessions

More than one administrator session can be running at the same time. These sessions could be using the web interface, command line interface, or a mixture of both. Be aware that if each administrator session attempts to modify the same configuration settings, changes made in one session will overwrite changes made in another session.

Session limits and timeouts

You can configure account session limits and inactivity timeouts, as described in Network Services.

Login history page (advanced account security)

If the system is in advanced account security mode, a **Login history** page is displayed immediately after logging in. This page shows the recent activity of the currently logged in account.

FindMe accounts

FindMe accounts are used by individuals in an enterprise to configure the devices and locations on which they can be contacted through their FindMe ID.

Each FindMe account is accessed using a username and password.

- If remote FindMe account authentication is selected, the Expressway administrator must set up FindMe groups to match the corresponding group names in the remote directory service.

Note Only the username and password details are managed remotely.

- All other properties of the FindMe account, such as the FindMe ID, devices and locations are stored in the local Expressway database.

See the Configuring FindMe accounts section for more information about defining FindMe account details and their associated FindMe devices and locations.

We recommend that you use Cisco TMS if you need to provision a large number of FindMe accounts. See Cisco TMS Provisioning Extension Deployment Guide for more details on configuring FindMe and user accounts.

Root account

The Expressway provides a root account which can be used to log in to the Expressway operating system. The **root** account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use an administrator account instead.

See the Using the Root Account section for more information.

Caution The pre-X8.9 default passwords of the **admin** and **root** accounts are well known. You must use strong passwords for these accounts. If your new system is on X8.9 or later, you must supply non-default passwords on startup.

More Information

See Configuring Administrator Accounts.

Configuring Password Security

The **Password security** page (**Users** > **Password security**) controls whether or not passwords for *local* accounts must meet a minimum level of complexity before they are accepted.

- If **Enforce strict passwords** is set to *On*, all subsequently configured passwords for qualifying accounts must conform to the following rules for what constitutes a strict password.
- If **Enforce strict passwords** is set to *Off*, no extra checks are made on passwords. The default is *Off*.

The minimum number of bits of entropy in generated passphrases is also configurable on this page, in the range 0 to 255 (the default is 6).

Note You can never set a blank password for any administrator account, regardless of this setting.

Scope of strict passwords

The **Enforce strict passwords** setting applies only to local accounts that are managed in Expressway itself:

- Local administrator accounts
- Local FindMe user accounts
- Local authentication database credentials (a list of valid usernames and passwords that are used when other devices are required to authenticate with the Expressway)

It does not affect any other passwords used on Expressway, such as LDAP/remotely stored administrator and FindMe credentials.

Note All passwords and usernames are case sensitive.

Non-configurable rules for strict passwords

The following password rules always apply when **Enforce strict passwords** is set to *On*, and they cannot be configured:

- Avoid multiple instances of the same characters (non-consecutive instances are checked)
- Avoid three or more consecutive characters such as “abc” or “123”
- Avoid dictionary words, or reversed dictionary words
- Avoid palindromes, such as “risetovotesir”

While creating or modifying passwords for administrator accounts, FindMe user accounts, and the local authentication database, if **Enforce strict passwords** is *On*, and the password has the same letters as the username in straight or reverse order in lower or upper case, an error message displays at the top of the page.

Configurable rules for strict passwords

The following properties of the password policy can be configured:

If **Enable custom forbidden password dictionary** is set to *On*, it allows the use of a custom forbidden password dictionary to perform strict password checks.

If **Enable custom forbidden password dictionary** is set to *Off*, no custom dictionary is utilized when performing strict password checks. Default is *Off*.

- Length must be at least 6 ASCII characters, but can be up to 255 (default 15)
- Number of numeric digits [0-9] may be between 0 and 255 (default 2)
- Number of uppercase letters [A-Z] may be between 0 and 255 (default 2)
- Number of lowercase letters [a-z] may be between 0 and 255 (default 2)
- Number of special characters [printable characters from 7-bit ASCII, for example, (space), @, $ etc.)] may be between 0 and 255 (default 2)
- Number of consecutive repeated characters allowed may be between 1 and 255 (the default 0 disables the check, so consecutive repeated characters are allowed by default; set it to 1 to prevent a password from containing any consecutive repeats)
- The minimum number of character classes may be between 0 and 4 (the default 0 disables the check). Character classes are digits, lowercase letters, uppercase letters, and special characters.

  You may experience precedence effects between the required number of character classes and the number of characters per class.

  For example: if you leave the default requirements of 2 characters of each class, there is an *implied* rule that 4 character classes are required. In this case any setting of **Minimum number of character classes** is irrelevant. Or, if you set the minimum number of character classes to 2, and the minimum number of characters required from each class to 0, then a password that contains characters from any two of the classes will suffice (presuming it meets the other criteria).

Password Encryption

All passwords configured on Expressway are stored securely in an encrypted or hashed form. This applies to the following items, which all have usernames and passwords associated with them:

- Default admin administrator account
- Any additional administrator accounts
- Local authentication database credentials (a list of valid usernames and passwords that are used when other devices are required to authenticate with the Expressway)
- Outbound connection credentials (used by the Expressway when required to authenticate with another system)
- LDAP server (used by the Expressway when binding to an LDAP server)

Local administrator account passwords are hashed using SHA512. Other passwords are stored in an encrypted format.

Web interface and CLI compared

When entering or viewing passwords using the web interface, you see placeholder characters instead of the characters you are typing.

When entering passwords using the command line interface, you type the password in plain text. However, after the command is executed, the password is displayed in its encrypted form with a *{cipher}* prefix. For example:

xConfiguration Authentication Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="

Maximum length of passwords

For each type of password, the maximum number of plain text characters that can be entered is shown in the table below.

Password type	Maximum length
Admin account	1024
Other local administrator accounts	1024
Local database authentication credentials	128
Outbound connection credentials	128
LDAP server	60
FindMe accounts	1024

Note When a password is encrypted and stored, it uses more characters than the original plain text version.

Forbidden Password Dictionary

Note If you have not configured the Forbidden password dictionary, clicking it displays a warning message,

```
This Expressway is not currently configured to use a custom forbidden password
dictionary.
```

Downloading Forbidden Password Dictionary

Step 1 Go to **Users** > **Forbidden password**.

Step 2 Click **Download dictionary** to download the current version of the dictionary to your local drive.

Uploading Forbidden Password Dictionary

Note

- Only **.txt** file is supported.
- Make sure you upload files along **/tmp/** path to keep the file upload process secure.

  For example, Consider the following command:

  ```
  xcommand Passworddictionarywrite
  ```

  Use **/tmp/** at the beginning of the path:

  ```
  xcommand Passworddictionarywrite /tmp/random_file
  ```

  If **/tmp/** is not specified, the following error message is displayed.

  ```
  PasswordDictionaryWriteCommandError: Forbidden password dictionary file
  path must start with /tmp/
  ```

Step 1 Go to **Users** > **Forbidden password**.

Step 2 Click **Choose File**.

Step 3 Select the dictionary file you want to upload from your local drive and click **Upload dictionary**.
Result: The new dictionary is uploaded and integrated into the application.

Updating Forbidden Password Dictionary

Step 1 Go to **Users** > **Forbidden password**.

Step 2 Click **Download dictionary**.

Download the current version of the dictionary and make necessary changes.

Step 3 Click **Choose File** and select the updated file.

Step 4 Click **Upload dictionary**.

The updated dictionary is uploaded and integrated into the application.

Generating Passphrase

Generate passphrase provides a random secure passphrase that is longer than a password and contains spaces in between words which increases security, without the cryptic series of letters, numbers, and symbols, improving usability. It prevents unauthorized users from decrypting them. The default length of the generated passphrase is 64.

Step 1 Go to **Maintenance** > **Tools** > **Generate Passphrase**

Step 2 A new **Generated passphrase** displays.

Configuring Administrator Accounts

The **Administrator accounts** page (**Users** > **Administrator accounts**) lists all the local administrator accounts on the Expressway.

In general, local administrator accounts are used to access the Expressway on its web interface or API interface, but are not permitted to access the CLI.

On this page you can:

- Create a new administrator account
- Change an administrator password
- Change the access level of an account: *Read-write*, *Read-only*, or *Auditor*
- Change the access scope of an account: *Web access*, *API access*, or both
- Delete, enable, or disable individual or multiple administrator accounts
- Nominate an emergency account

Editing Administrator Account Details

You can edit the details for the default administrator account and for additional local administrator accounts.

Step 1 Go to **Users** > **Administrator accounts**.

Step 2 Under **Actions** for the relevant administrator account, click **Edit user**.

A new page is displayed, where you can edit all fields for the selected administrator account except for the password.

Changing the Password

Step 1 Go to **Users** > **Administrator accounts**.

Step 2 Under **Actions** for the relevant administrator account, click **Change password**.

A new page is displayed, where you can change the password for the selected administrator account.

Step 3 Go to **Related tasks** section and click **Generate passphrase**.

A new passphrase displays on the **Generated passphrase** page.

Step 4 Enter or copy paste the newly generated passphrase in **New password** field and **Confirm new password** field text box.

Step 5 Enter your **Current password** to authorize the password change process.

Step 6 Click **Save**.

A message `Password changed successfully` displays.

About the Administrator Account and Field References

This default local administrator "admin" account has full *Read-write* access and can access the Expressway using the web UI, the API interface, or the CLI.

The username for this account is **admin** (all lower case).

Note Presently, only the built-in **admin** user has access to CLI. From 14.0.1 and later, Multiple Admin Accounts and Groups can have CLI access. Administrator Users can provide this access through a User Interface. Similarly, it also allows Administrator Users to toggle access between the CLI and REST API.

Before X8.9, the default password was **TANDBERG** (all upper case). From X8.9 onwards, new systems run a secure install wizard on startup, so that you can provide new passwords before the system is connected to the network.

You cannot delete, rename, or disable **admin** and you cannot change its access level from *Read-write*, but you can disable its web and API access.

If your system was upgraded from a pre-X8.9 version, you may need to change the password. Choose a strong password, particularly if administration over IP is enabled.

If you forget the password for the **admin** account, you can log in as another administrator account with read-write access and change the password for the **admin** account. If there are no other administrator accounts, or you have forgotten those passwords as well, you can still reset the password for the **admin** account providing you have physical access to the Expressway. See Resetting Forgotten Passwords for details.

Administrator account fields reference

Field	Description	Usage tips
Name	The username for the administrator account.	Some names such as "root" are reserved. Local administrator account user names are case sensitive.

Field	Description	Usage tips
Access level	The access level of the administrator account: *Read-write*: Allows all configuration information to be viewed and changed. This provides the same rights as the default **admin** account. *Read-only*: Allows status and configuration information to be viewed only and not changed. Some pages, such as the **Upgrade** page, are blocked to read-only accounts. *Auditor*: Allows access to the **Event Log**, **Configuration Log**, **Network Log**, **Alarms** and **Overview** pages only. Default: *Read-write*	The access permissions of the currently logged in user are shown in the system information bar at the bottom of each web page. The access level of the default **admin** account cannot be changed from *Read-write*.
Password	The password that this administrator will use to log in to the Expressway.	All passwords on the Expressway are encrypted, so you only see placeholder characters here. When entering passwords, the bar next to the **Password** field changes color to indicate the complexity of the password. You can configure the complexity requirements for local administrator passwords on the Configuring Password Security page (**Users** > **Password security**). You cannot set blank passwords. **Note** While creating or modifying a password, for Administrator Accounts, Local authentication database, and FindMe users, if "**Enforce strict passwords**" is ON, and the password has the same letters as the username in straight or reverse order (in lower or upper case), an error message displays at the top of the page.
New password	Enter a new password for the account.	This field only appears when you are changing a password.
Confirm password	Re-enter the password for the account.	This field only appears when you create an account or when you change its password.

Field	Description	Usage tips
Emergency account	Select *Yes* to use this account as the emergency account. You must use an enabled local administrator account that has read-write access and web access.	You may only have one emergency account, and you can use this account to gain access to the Expressway even if it does not allow local authentication. The purpose of this account is to help you work around being locked out of the system when remote authentication is not available.
Web access	Select whether this account is allowed to log in to the system using the web interface. Default: *Yes*	
Force password reset	If you select Yes, then the new user must create a new password when they log in. Default: *No*	
API access	Select whether this account is allowed to access the system's status and configuration using the Application Programming Interface (API). Default: *Yes*	This controls access to the XML and REST APIs by systems such as Cisco TMS.
State	Select whether the account is *Enabled* or *Disabled*. Disabled accounts are not allowed to access the system.	
Your current password	Enter your own, current password here if the system requires you to authorize a change.	To improve security, the system requires that administrators enter their own passwords when creating an account or changing a password.

Viewing Active Administrator Sessions

The **Active administrator sessions** page (**Users** > **Active administrator sessions**) lists all administrator accounts that are currently logged in to this Expressway.

It displays details of their session including their login time, session type, IP address and port, and when they last accessed this Expressway.

You can terminate active web sessions by selecting the required sessions and clicking **Terminate session**.

You may see many sessions listed on this page if a zero **Session time out** value is configured. This typically occurs if an administrator ends their session by closing down their browser without first logging out of the Expressway.

Configuring Remote Account Authentication Using LDAP

The **LDAP configuration** page (**Users** > **LDAP configuration**) is used to configure an LDAP connection to a remote directory service for administrator account authentication.

The configurable options are:

Field	Description	Usage tips
Remote account authentication: This section allows you to enable or disable the use of LDAP for remote account authentication.		
Administrator authentication source	Defines where administrator login credentials are authenticated. *Local only*: Credentials are verified against a local database stored on the system. *Remote only*: Credentials are verified against an external credentials directory. *Both*: Credentials are verified first against a local database stored on the system, and then if no matching account is found the external credentials directory is used instead. The default is *Local only*.	*Both* allows you to continue to use locally-defined accounts. This is useful while troubleshooting any connection or authorization issues with the LDAP server. You cannot log in using a locally-configured administrator account, including the default **admin** account, if *Remote only* authentication is in use. **Note** Do not use *Remote only* if Expressway is managed by Cisco TMS.
LDAP server configuration: This section specifies the connection details to the LDAP server.		
FQDN address resolution	Defines how the LDAP server address is resolved. *SRV record*: DNS SRV record lookup. *Address record*: DNS A or AAAA record lookup. *IP address*: Entered directly as an IP address. The default is *Address record*. If you use SRV records, ensure that *_ldap._tcp.<domain> records* use the standard LDAP port 389. The Expressway does not support other port numbers for LDAP. To use LDAPS with SRV, the AD server must support the STARTTLS extension. (If you want to do LDAPS using port 636, you need to use an address record for FQDN resolution, and connect directly to port 636.)	The SRV lookup is for _ldap._tcp records. If multiple servers are returned, the priority and weight of each SRV record determines the order in which the servers are used.

Field	Description	Usage tips
Host name and **Domain** or **Server address**	The way in which the server address is specified depends on the **FQDN address resolution** setting: *SRV record*: Only the **Domain** portion of the server address is required. *Address record*: Enter the **Host name** and **Domain**. These are then combined to provide the full server address for the DNS address record lookup. *IP address*: The **Server address** is entered directly as an IP address.	If using TLS, the address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.
Port	The IP port to use on the LDAP server.	The Expressway *only* supports ports 636 or 3269 for LDAP Encrypted connections.
Encryption	Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS). • *TLS*: Uses TLS encryption for the connection to the LDAP server. • *Off*: No encryption is used. The default is *TLS*. For more information, see Configuring Minimum TLS Version and Cipher Suites.	When TLS is enabled, the LDAP server's certificate must be signed by an authority within the Expressway's trusted CA certificates file. Click **Upload a CA certificate file for TLS** (in the **Related tasks** section) to go to the Managing the Trusted CA Certificate List page.
Certificate revocation list (CRL) checking	Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server. *None*: No CRL checking is performed. *Peer*: Only the CRL associated with the CA that issued the LDAP server's certificate is checked. *All*: All CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked. The default is *None*.	If you are using revocation lists, any required CRL data must also be included within the CA certificate file.
Authentication configuration: This section specifies the Expressway's authentication credentials to use when binding to the LDAP server.		

Field	Description	Usage tips
Bind DN	The distinguished name (case insensitive) used by the Expressway when binding to the LDAP server. It is important to specify the DN in the order cn=, then ou=, then dc= **Note** Make sure that you provide LDAP users with the least possible privileges.	Any special characters within a name must be escaped with a backslash as per the LDAP standard (*RFC 4514*). Do not escape the separator character between names. The bind account is usually a read-only account with no special privileges.
Bind password	The password (case sensitive) used by the Expressway when binding to the LDAP server.	The maximum plaintext length is 60 characters, which is then encrypted.
SASL	The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. *None*: No mechanism is used. *DIGEST-MD5*: The DIGEST-MD5 mechanism is used. The default is *DIGEST-MD5*.	Enable Simple Authentication and Security Layer if it is company policy to do so.
Bind username	Username of the account that the Expressway will use to log in to the LDAP server (case sensitive). Only required if SASL is enabled.	Configure this to be the sAMAccountName; Security Access Manager Account Name (in AD this is the account's user logon name).
Directory configuration: This section specifies the base distinguished names to use when searching for account and group names.		
Base DN for accounts	The ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	The Base DN for accounts and groups must be at or below the dc level (include all dc= values and ou= values if necessary). LDAP authentication does not look into sub dc accounts, only lower ou= and cn= levels.
Base DN for groups	The ou= and dc= definition of the Distinguished Name where a search for groups should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	If no **Base DN for groups** is specified, then the Base DN for accounts will be used for both groups and accounts.
Nested subgroup search depth	Used to limit the depth of groups for the LDAP search.	For optimal search performance, define the top-level group for the remote administrator as an (administrator) group in Expressway and set the search depth to "1".

Field	Description	Usage tips
Skip looking up all the members	Used to disable or enable member lookup of an administrator group during the authentication search process. The default is "*Yes*" - skip the member lookup.	We recommend keeping this setting as "*Yes*" if the configured groups have relatively high numbers of members. However, for deployments where the configured groups have relatively few members, setting it to "*No*" (do member lookup) may help to reduce authentication latency.

Checking the LDAP Server Connection Status

The status of the connection to LDAP server is displayed at the bottom of the page.

State = **Available**

No error messages are displayed.

State = Failed

The following error messages may be displayed:

Error message	Reason / resolution
DNS unable to do reverse lookup	Reverse DNS lookup is required for SASL authentication. **Note** To facilitate reverse lookup, give the domain in the form of 152.50.10.in-addr.arpa (the subnet of addresses would be 10.50.152.0/24) and the target DNS server in the address. This sends all requests in the subnet to the target DNS server instead of the default server.
DNS unable to resolve LDAP server address	Check that a valid DNS server is configured, and check the spelling of the LDAP server address.
Failed to connect to LDAP server. Check server address and port	Check that the LDAP server details are correct.
Failed to setup TLS connection. Check your CA certificate	CA certificate, private key and server certificate are required for TLS.
Failure connecting to server. Returned code<return code>	Other non-specific problem.
Invalid Base DN for accounts	Check **Base DN for accounts**; the current value does not describe a valid part of the LDAP directory.
Invalid server name or DNS failure	DNS resolution of the LDAP server name is failing.

Error message	Reason / resolution
Invalid bind credentials	Check **Bind DN** and **Bind password**, this error can also be displayed if SASL is set to *DIGEST-MD5* when it should be set to *None*.
Invalid bind DN	Check **Bind DN**; the current value does not describe a valid account in the LDAP director. This failed state may be wrongly reported if the **Bind DN** is 74 or more characters in length. To check whether there is a real failure or not, set up an administrator group on the Expressway using a valid group name. If Expressway reports "saved" then there is not a problem (the Expressway checks that it can find the group specified). If it reports that the group cannot be found then either the **Bind DN** is wrong, the group is wrong or one of the other configuration items may be wrong.
There is no CA certificate installed	CA certificate, private key and server certificate are required for TLS.
Unable to get configuration	LDAP server information may be missing or incorrect.

Configuring Administrator Groups

The **Administrator groups** page (**Users** > **Administrator groups**) lists all the administrator groups that have been configured on the Expressway, and lets you add, edit and delete groups.

Administrator groups only apply if Configuring Remote Account Authentication Using LDAP is enabled.

When you log in to the Expressway web interface, your credentials are authenticated against the remote directory service and you are assigned the access rights associated with the group to which you belong. If the administrator account belongs to more than one group, the highest level permission is assigned.

The configurable options are:

Field	Description	Usage tips
Name	The name of the administrator group. It cannot contain any of the following characters: / \ [ ] : ; | = , + * ? > < @ "	The group names defined in the Expressway must match the group names that have been set up in the remote directory service to manage administrator access to this Expressway.

Field	Description	Usage tips
Access level	The access level given to members of the administrator group: *Read-write*: Allows all configuration information to be viewed and changed. This provides the same rights as the default **admin** account. *Read-only*: Allows status and configuration information to be viewed only and not changed. Some pages, such as the **Upgrade** page, are blocked to read-only accounts. *Auditor*: Allows access to the **Event Log, Configuration Log**, **Network Log**, **Alarms** and **Overview** pages only . *None*: No access is allowed. Default: *Read-write*	If an administrator belongs to more than one group, it is assigned the highest level permission for each of the access settings across all of the groups to which it belongs (any groups in a disabled state are ignored). See Determining the access level for accounts that belong in multiple groups below for more information.
Web access	Determines whether members of this group are allowed to log in to the system using the web interface. Default: *Yes*	
API access	Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API). Default: *Yes*	This controls access to the XML and REST APIs by systems such as Cisco TMS.
State	Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups.	If an administrator account belongs to more than one administrator group with a combination of both *Enabled* and *Disabled* states, their access will be *Enabled*.

Determining the access level for accounts that belong in multiple groups

If an administrator belongs to groups with different levels of access, the highest level of access is granted. Any groups in a disabled state are ignored.

For example, if the following groups were configured:

Group name	Access level	Web access	API access
Administrators	Read-write	-	-
Region A	Read-only	Yes	-
Region B	Read-only	-	Yes
Region C	Read-only	Yes	Yes

The following table shows examples of the access permissions that would be granted for accounts that belong in one or more of those groups:

Groups belonged to	Access permissions granted
Administrators and **Region A**	read-write access to the web interface but no API access
Administrators and **Region B**	read-write access to the API interface, but no web interface access
Administrators and **Region C**	read-write access to the web and API interfaces
Region A only	read-only access to the web interface and no API access

Resetting Forgotten Passwords

You can reset any account password by logging in to the Expressway as the default **admin** account or as any other administrator account that has read-write access. If this is not possible you can reset the **admin** or **root** password via the console.

Note Stored configuration and data will not be affected when you reset your password.

Changing an Administrator Account Password Through the Web Interface

You can change the password for the default administrator account and for additional local administrator accounts.

Step 1 Go to **Users** > **Administrator accounts**.

Step 2 Under **Actions** for the relevant administrator account, click **Change password**.

A new page is displayed, where you can change the password for the selected administrator.

Step 3 Enter the new password and confirm it.

Note You must also enter the password for the administrator account with which you are currently logged in to authorize the password change.

Resetting the Root or Admin Password Through a Serial Connection

On a hardware Expressway, reset the **admin** or **root** password as follows:

Step 1 Connect a PC to the Expressway using the serial cable. Serial port / console access is always enabled for one minute following a restart, even if it is normally disabled.

Step 2 Restart the Expressway.

Step 3 Log in from the PC with the username **`pwrec`**. No password is required.

Step 4 If the administrator account authentication source is set to *Remote*, you are given the option to change the setting to *Both*; this will allow local administrator accounts to access the system.

Step 5 Select the account to be changed (**root** or **admin**).

Step 6 You are prompted for a new password.

What to do next

The **pwrec** account is only active for one minute following a restart. After that time you will need to restart the system again to change the password.

Resetting Root or Admin Password via vSphere

If you have forgotten the password for either an administrator account or the **root** account and you are using a VM (Virtual Machine) Expressway, you can reset it using the following procedure:

Step 1 Open the vSphere client.

Step 2 Click on the link **Launch Console**.

Step 3 Reboot the Expressway.

Step 4 In the vSphere console log in with the username **`pwrec`**. No password is required.

Step 5 When prompted, select the account (*root* or the username of the administrator account) whose password you want to change.

Step 6 You are prompted for a new password.

What to do next

The **pwrec** account is only active for one minute following a reboot. After that time you will need to reboot the system again to reset the password.

Using the Root Account

The Expressway provides a root account which can be used to log in to the Expressway operating system. This account has a username of **root** (all lower case)) and set the password of your choice when prompted. An alarm is displayed on the web interface and the CLI if the **root** account has the default password set.

Note The **root** account may allow access to sensitive information and it should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the **admin** account instead.

Changing the Root Account Password

Step 1 Log in to the Expressway as **root** using the existing password. By default you can only do this using a serial connection or SSH.

Step 2 Type the command **`passwd`**.

You will be asked for the new password.

Step 3 Enter the new password and when prompted, retype the password.

Step 4 Type **`exit`** to log out of the root account.

Accessing the Root Account Over SSH

Note
- The root account can be accessed over a serial connection or SSH only.
- If you have disabled SSH access while logged in using SSH, your current session will remain active until you log out, but all future SSH access will be denied.

You can enable and disable access to the root account using SSH.

Step 1 Log in to the Expressway as **root**.

Step 2 Type one of the following commands:

- **rootaccess --ssh on** - To enable access using SSH
- **rootaccess --ssh off** - To disable access using SSH

Step 3 Type **`exit`** to log out of the root account.

Setting the Pwrec Account Password

As of X14.0 release, you can set a password for pwrec account through command line interface only.

Important Once a password is set, the account will always require a password. Currently, there's no way to reset the password.

To set a password:

- Log in as root via SSH, or through the physical appliance
- Set the password using "passwd pwrec".
- You'll be prompted to enter a new password and retype it to confirm.
- If both the passwords match a message, "passwd: password updated successfully" displays.
    - If the passwords don't match a message, Sorry", passwords don't match" displays.

Managing SSO tokens

Note This page applies to standard OAuth tokens configured by the **Authorize by OAuth token** setting. It does not apply to self-describing OAuth tokens (configured by **Authorize by OAuth token with refresh**).

1. **View the list of users who currently hold SSO tokens**: Go to **Users** > **SSO token holders** to view the list of users who currently hold SSO tokens. This page can help you troubleshoot issues related to single sign-on for a particular user.
2. **Purge tokens from all holders**: You can also use this page to **Purge tokens from all holders**. This option is probably disruptive for your users so make sure you need it before you proceed. You may need it, for example, if you know your security is compromised, or if you are upgrading internal or edge infrastructure.

Managing the tokens of a particular user

Step 1 [Optional] Filter by a substring of the username to return a smaller list.

You may need this if there are many usernames in the list, because a long list spans multiple pages of up to 200 usernames each.

Step 2 Click a username to see the detail of the tokens held by that user.

The **SSO tokens for user <*Username*>** page appears, listing details of the tokens issued to that user. The details include the token issuer and expiry.

Step 3 [Optional] Click **Delete these tokens** if you want the user's identity to be confirmed before they continue to access the UC services.

The next time the user's client attempts to access UC services via this Expressway-C, the client will be redirected to the IdP with a new, signed request. The user may need to reauthenticate at the IdP, so that it can assert their identity to the Expressway-C. The user can then be issued with new tokens where authorized.