Manage Admins

Setting up who in your organization's security and operations teams (ie, which Admins) can view and edit configurations in the Command Center.

Updated on

ON THIS PAGE:

For security reasons, SonicWall Cloud Secure Edge (CSE) handles Admins and Users completely separately.
- **Admins** manage access control security policies via the Command Center Web Console and API.
- **Users** use their Devices to access Services that are secured by CSE's enforcement components. To manage users, refer to the articles on configuring IDPs.

Note: Cloud Secure Edge orgs are now provisioned in MySonicWall. Use MySonicWall to add and manage admins. Admins assigned via MySonicWall are SAML-Only admins.

Account Types

CSE categorizes administrative accounts by their **Account Type**. CSE provides two types of admin accounts:

- Local
- SAML-Only

The table below lists the possible permissions and attributes for CSE account types.

Permission/Attribute	Local	SAML-Only
Available if Local Admin is enabled	✔	
Available if SAML Single Sign On is enabled		✔
Created via Command Center (**Settings** > **Manage Admins**)	✔	

Permission/Attribute	Local	SAML-Only
Created just-in-time once authenticated with SAML Single Sign On Provider		✔
Can use local account password to log in to the Command Center	✔	
Can use SAML Single Sign On to log into the Command Center	✔	✔
Can generate API Keys for API access	✔	✔
Can generate Personal Refresh Token for API access	✔	
Can create Local administrator accounts (if account has Admin or Owner profile)	✔	
Can delete administrator accounts (if account has Admin or Owner profile)	✔	

Administrator Profiles

Every admin (Local or SAML-Only) is assigned a **profile** that is associated with a single **privilege level**. CSE provides several profiles, listed here in order of privilege:

- Owner (every organization must have at least one Owner)
- Admin
- ServiceAuthor
- PolicyAuthor
- EventWriter
- ReadOnly

The table below lists the permissions associated with the admin privilege levels:

Permissions	Owner	Admin	ServiceAuthor	PolicyAuthor	EventWriter	ReadOnly
Create/Update/Delete Owners	✔					
Create/Update/Delete Non-Owner Admins	✔	✔				
Manage Organization Settings	✔	✔				
Manage Services	✔	✔	✔			
Manage Roles & Policies	✔	✔		✔		
Manage Trust Profiles	✔	✔	✔	✔		
Submit Events	✔	✔	✔	✔	✔	✔
View Configurations (Services, Policies,	✔	✔	✔	✔	✔	✔

Permissions	Owner	Admin	ServiceAuthor	PolicyAuthor	EventWriter	ReadOnly
Events, Directory etc)						

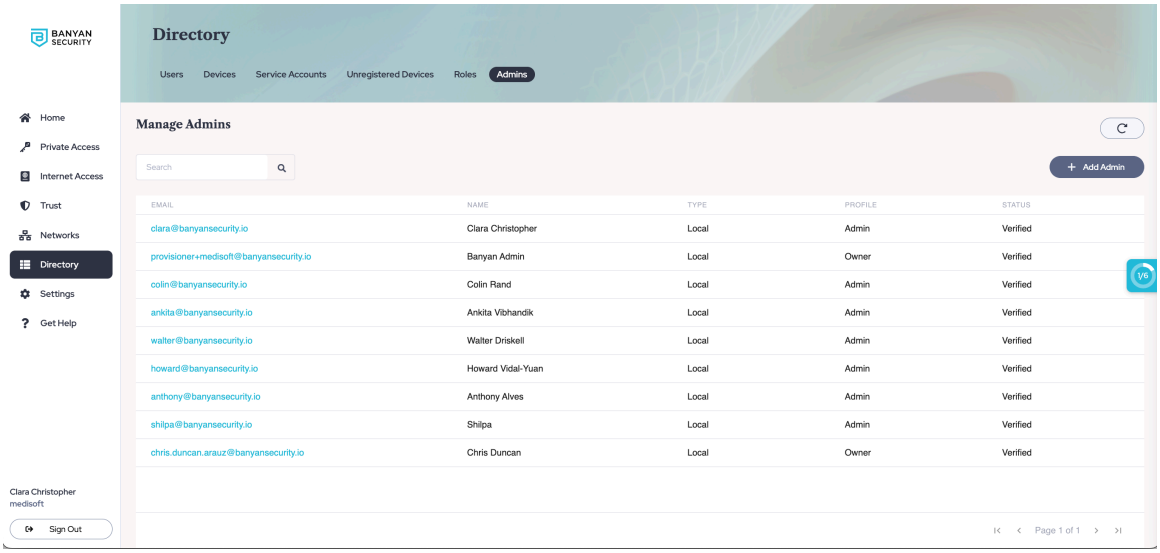
When a SAML-Only account is created just-in-time, it is assigned a ReadOnly profile by default. Any administrator with Admin privilege can change the account's profile.

Note: ReadOnly Admins cannot view System Logs, which provide a time-stamped log of administrators' actions in the CSE console, so that their previous actions can be reviewed and understood for auditing purposes.

List of Admins

View the list of administrators who have access to your Organization in the Command Center by navigating to **Directory** > **Admins**.

Admins with SAML-only accounts will not show up in the Manage Admins users list until they have logged into the Command Center for the first time.



Local Account Passwords and Lockout Threshold

Local admins can use a local account password to log into the Command Center (unlike SAML-Only administrators, who must authenticate via their SSO Provider).

CSE's password policy requires all local accounts to have complex passwords that meet the following requirements:

- 8 or more characters;
- contains at least 1 uppercase letter;
- contains at least 1 lowercase letter;
- contains at least 1 digit; and
- contains at least 1 symbol

Local admin accounts are also configured with a lockout threshold (based on failed log-ons and password resets) to ensure that brute force attacks cannot compromise the account. Finally, a robust audit mechanism alerts the CSE operations team when a series of failed log-ons or password resets occur in a given environment.

For more customizable admin authentication and alerting policies, you should enable SAML Single Sign On.

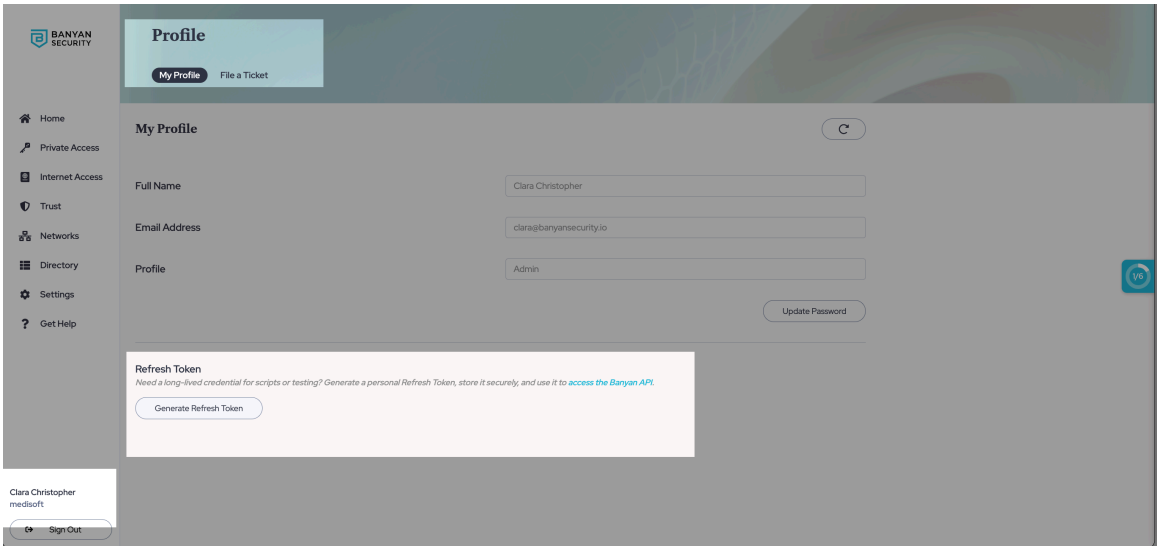
Deleting Admin Accounts and Decommissioning an Organization

In order to delete admin accounts, you need to be an administrator with an Admin profile. In order to delete a SAML-Only admin, you must first remove them from your SAML Single Sign On Provider, and then you can delete them in CSE. Note that the default admin account is given a ReadOnly profile and cannot delete other admin accounts.

An organization must have at least 1 administrator with the Owner profile at all times; thus, you cannot delete every single admin account associated with an organization. Only the CSE Operations Team can delete the final administrator account with Owner profile and completely decommission an organization. Contact CSE Support if you need to do this.

Personal Refresh Tokens

Local Admins can generate Personal Refresh Tokens for automation workflows. To generate a personal Refresh Token, navigate to your **My Profile** tab (by selecting your user name in the bottom left corner of the Command Center), and then select **Generate Refresh Token**.



The Refresh Token gives you full API access to your account - please store these tokens securely and do not provide them to a third party. The Command Center provides one Refresh Token per user account - it never expires but you can revoke the Refresh Token at any time.

Access Tokens to interact with the CSE (formerly Banyan) API can be obtained by submitting your Refresh Token.

To revoke a Refresh Token, navigate to the **My Profile** tab, and then select **Revoke Token**.

SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts

Components

Release Notes

Guides

Quick Start Guides

Solutions

Feature Guides

API Guide