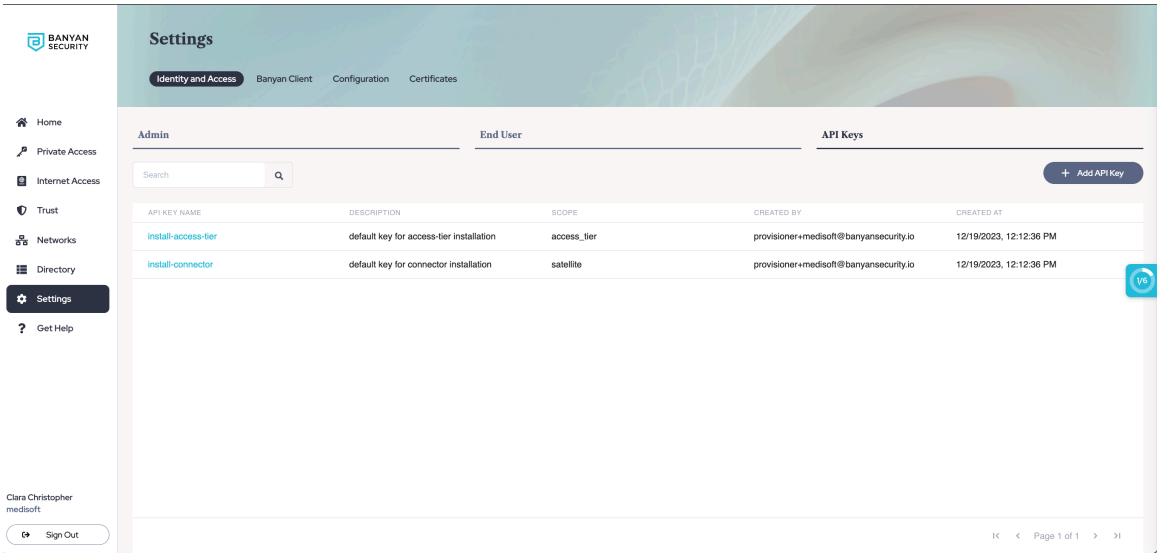
Manage API Keys

Updated on

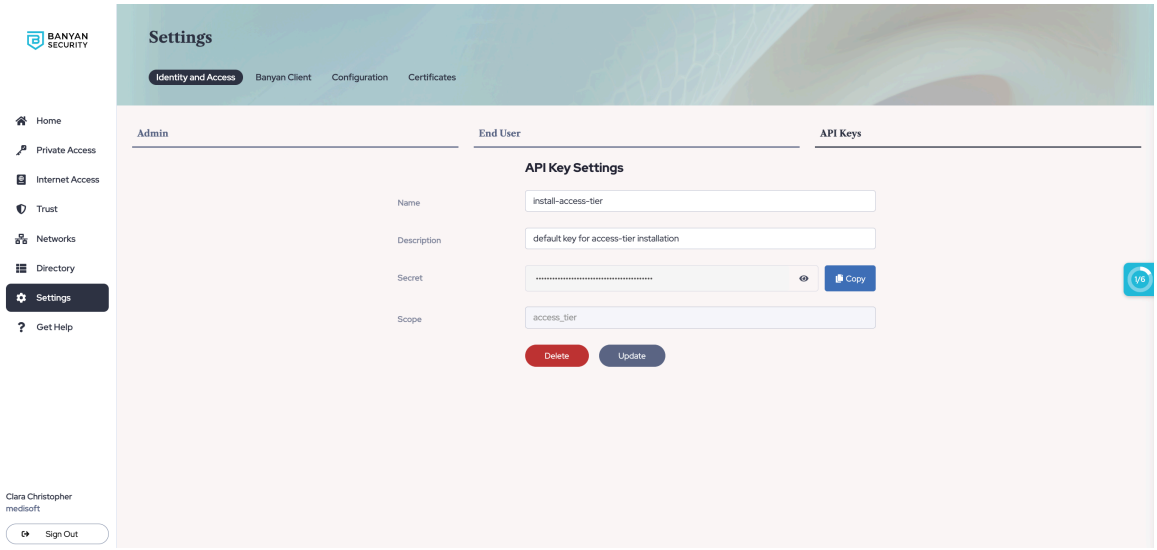
ON THIS PAGE:

API Keys

Admins can create and manage API keys for programmatic access to the Command Center REST APIs. Navigate to **Settings** > **Identity and Access** > **API Keys** to see the API keys for your org:



Every API key object has a **Secret** value that grants access to the Command Center REST APIs, and should be stored securely.



API Key Privilege Levels

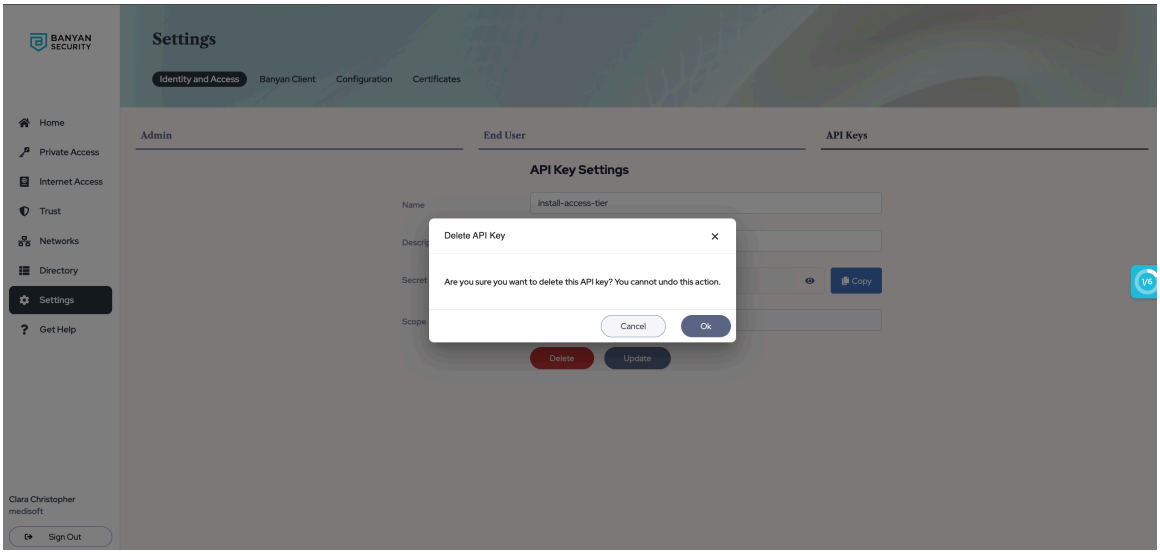
API keys can be issued with the Admin privilege levels - `Admin`, `ServiceAuthor`, `PolicyAuthor`, `EventWriter`, `ReadOnly` - or at more specific scopes - `satellite`, `access_tier`, etc.

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, Events, Directory etc)	✔	✔	✔	✔	✔	✔

Revoking API Keys

API keys can be revoked at any time by deleting them. Any automation scripts that use a deleted API key will stop working immediately.



SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts
Components
Release Notes

Guides

Quick Start Guides
Solutions
Feature Guides
API Guide