



Falcon Management

12/08/2025

1. Falcon Management

1.1. Falcon Console User Guide

- 1.1.1. Overview
- 1.1.2. Supported browsers
- 1.1.3. Accessing the Falcon console
- 1.1.4. Falcon console navigation
 - 1.1.4.1. Navigation bar
 - 1.1.4.2. CID switcher
 - 1.1.4.3. Falcon console menu
 - 1.1.4.3.1. Menu status flags
 - 1.1.4.4. Falcon console bookmarks
 - 1.1.4.4.1. Create bookmarks
 - 1.1.4.4.2. Rename bookmarks
 - 1.1.4.4.3. Remove bookmarks
 - 1.1.4.4.4. Remove all bookmarks
 - 1.1.4.5. Central search
 - 1.1.4.5.1. Search input
 - 1.1.4.5.2. What is searched?
 - 1.1.4.5.3. Search suggestions
 - 1.1.4.5.4. Search results
 - 1.1.4.6. Falcon notifications
- 1.1.5. Overview of key features
 - 1.1.5.1. Comments and copy / paste
 - 1.1.5.2. Customize columns
 - 1.1.5.3. Data export
 - 1.1.5.4. Filter bar
 - 1.1.5.5. Data from partner apps
- 1.1.6. Profile settings

1.2. Falcon Status Dashboard

- 1.2.1. Overview
- 1.2.2. Understand the dashboard
 - 1.2.2.1. Feature name
 - 1.2.2.2. Status
 - 1.2.2.3. Details
 - 1.2.2.3.1. Tech Alerts
 - 1.2.2.4. Actions

1.3. Host and Host Group Management

- 1.3.1. Requirements
- 1.3.2. Managing Hosts
 - 1.3.2.1. Viewing host overview info
 - 1.3.2.2. Navigating the Host Management page
 - 1.3.2.2.1. Find a host
 - 1.3.2.2.2. View a host's summary panel
 - 1.3.2.2.3. Host timeline
 - 1.3.2.2.3.1. Host states and events
 - 1.3.2.2.3.2. Modifying the host timeline
 - 1.3.2.2.3.3. Events list
 - 1.3.2.3. Export host data
 - 1.3.2.3.1. Quick exports
 - 1.3.2.3.2. Configure exports
 - 1.3.2.3.3. Download export reports
 - 1.3.2.3.4. Configure export templates
 - 1.3.2.3.5. Edit export templates
 - 1.3.2.3.6. Delete export templates
 - 1.3.2.4. View content update states
 - 1.3.2.5. Managing inactive and duplicate hosts
 - 1.3.2.5.1. Understanding host hide and delete actions
 - 1.3.2.5.1.1. Hiding mobile hosts
 - 1.3.2.5.2. Host retention policies
 - 1.3.2.5.2.1. Host retention policy assignment and precedence
 - 1.3.2.5.2.2. Create a host retention policy
 - 1.3.2.5.2.3. Duplicate a host retention policy
 - 1.3.2.5.2.4. Manage settings for a host retention policy
 - 1.3.2.5.2.5. Manage host retention policy precedence
 - 1.3.2.5.2.6. View a host's retention info
 - 1.3.2.5.3. Manually hide a host
 - 1.3.2.5.4. Restore a host
 - 1.3.2.6. Changing a host's network containment status
 - 1.3.2.7. Disabling detections on a host
- 1.3.3. Managing host groups
 - 1.3.3.1. Planning dynamic host groups
 - 1.3.3.1.1. Using standard attributes
 - 1.3.3.1.2. Group hosts using tags
 - 1.3.3.1.2.1. Falcon grouping tags
 - 1.3.3.1.2.2. Sensor grouping tags
 - 1.3.3.1.2.3. Third-party tags
 - 1.3.3.1.2.4. Adding Falcon grouping tags from the host summary panel
 - 1.3.3.1.2.5. Removing Falcon grouping tags from the host summary panel
 - 1.3.3.1.2.6. Adding Falcon grouping tags in bulk
 - 1.3.3.1.2.7. Removing Falcon grouping tags in bulk
 - 1.3.3.2. Find a host group
 - 1.3.3.3. View host group details
 - 1.3.3.3.1. View and manage assigned policies
 - 1.3.3.3.2. View assigned exclusions
 - 1.3.3.4. Create a host group
 - 1.3.3.5. Assign hosts to a host group
 - 1.3.3.5.1. Assign hosts to a dynamic group
 - 1.3.3.5.2. Assign hosts to a static group
 - 1.3.3.5.3. Remove hosts from a static group
 - 1.3.3.5.4. Manage host group assignments from the Hosts page
 - 1.3.3.5.4.1. Add or remove a host from a static group
 - 1.3.3.5.4.2. Add or remove multiple hosts from a static group
 - 1.3.3.6. Deleting a host group
- 1.3.4. Protecting your CID with installation tokens
 - 1.3.4.1. Before you begin
 - 1.3.4.2. Planning your installation tokens
 - 1.3.4.2.1. Example token lifecycle
 - 1.3.4.2.2. How tokens work
 - 1.3.4.3. Managing your installation tokens
 - 1.3.4.3.1. Creating installation tokens
 - 1.3.4.3.2. Editing installation tokens
 - 1.3.4.3.3. Revoking installation tokens
 - 1.3.4.3.4. Restoring revoked installation tokens
 - 1.3.4.4. Enabling or disabling Require tokens
 - 1.3.4.5. Installing sensors with installation tokens
 - 1.3.4.6. Reviewing tokens and actions
 - 1.3.4.7. Troubleshooting installation tokens
 - 1.3.4.7.1. Installations fail with new tokens
 - 1.3.4.7.2. Log contents when a Windows sensor installation fails

1.4. Policies in Falcon

- 1.4.1. Overview
- 1.4.2. How policies work
 - 1.4.2.1. Policy precedence and default policies
- 1.4.3. Manage policies in the Falcon console
 - 1.4.3.1. Policy details pages
 - 1.4.3.1.1. Assigned host groups
 - 1.4.3.1.2. Host group policy assignment details

1.5. Falcon Browser Extension

- 1.5.1. Overview
- 1.5.2. Falcon browser extension v2

Falcon Management

- 1.5.2.1. Requirements: Falcon browser extension v2
- 1.5.2.2. Before you begin
- 1.5.2.3. Setup: Falcon browser extension v2
 - 1.5.2.3.1. Custom installation: Mac
 - 1.5.2.3.1.1. Create a browser extension policy
 - 1.5.2.3.1.2. Install the Falcon browser extension and the Falcon sensor
 - 1.5.2.3.2. Custom installation: Windows
 - 1.5.2.3.2.1. Create a browser extension policy
 - 1.5.2.3.2.2. Install the Falcon browser extension and the Falcon sensor
 - 1.5.2.3.3. Automatic installation: Windows
- 1.5.2.4. Configure Falcon browser extension v2 policy settings
 - 1.5.2.4.1. Manage Falcon browser extension settings related to Data Protection
- 1.5.3. Falcon browser extension v1
 - 1.5.3.1. Requirements: Falcon browser extension v1
 - 1.5.3.2. Setup: Falcon browser extension v1
 - 1.5.3.2.1. Upgrade from browser extension v1
- 1.6. Falcon Notifications
 - 1.6.1. Overview
 - 1.6.1.1. Falcon notifications comparison
 - 1.6.2. Standard Incident and detection notification emails
 - 1.6.2.1. Requirements
 - 1.6.2.2. Planning standard incident and detection notification email recipients
 - 1.6.2.3. Managing standard incident and detection notification email recipients
 - 1.6.3. OverWatch incident email notifications
 - 1.6.3.1. Requirements:
 - 1.6.3.2. Understanding notifications from OverWatch
 - 1.6.4. Intelligence news and reports
 - 1.6.4.1. Overview
 - 1.6.4.2. Requirements
 - 1.6.5. Falcon MalQuery Monitoring Rule results
 - 1.6.5.1. Overview
 - 1.6.5.2. Requirements
- 1.7. Detection Attribute Management
 - 1.7.1. Overview
 - 1.7.2. Requirements
 - 1.7.3. Setup
 - 1.7.4. Managing detection attributes
 - 1.7.4.1. Configure detection attributes
 - 1.7.4.2. View and manage detections attribute templates
 - 1.7.4.2.1. View detections attribute templates
 - 1.7.4.2.2. Edit detections attribute templates
 - 1.7.4.2.3. Delete detections attribute templates
 - 1.7.4.2.4. See detections affected by a detections attribute template
- 1.8. Users and Roles
 - 1.8.1. User Management
 - 1.8.1.1. Overview
 - 1.8.1.2. Requirements
 - 1.8.1.3. Understanding CIDs
 - 1.8.1.3.1. Home CID
 - 1.8.1.3.2. Accessing multiple CIDs
 - 1.8.1.4. Understanding user accounts
 - 1.8.1.4.1. Unique email address
 - 1.8.1.4.2. Approved domains
 - 1.8.1.5. Understanding access control
 - 1.8.1.5.1. Controlling access in the console with user roles
 - 1.8.1.5.1.1. Use temporary roles to grant and revoke access
 - 1.8.1.5.1.2. Role assignment types in Flight Control
 - 1.8.1.5.2. Controlling access to data with FGA
 - 1.8.1.5.2.1. FGA for hosts and Flight Control
 - 1.8.1.6. Managing users
 - 1.8.1.6.1. Add users
 - 1.8.1.6.1.1. Add a user in a standalone CID or child CID
 - 1.8.1.6.1.2. Add a user from the Flight Control parent CID
 - 1.8.1.6.2. Viewing the users list
 - 1.8.1.6.3. Viewing the User details page
 - 1.8.1.6.4. Manage a user's access
 - 1.8.1.6.4.1. Update user access
 - 1.8.1.6.4.2. Update host group assignments using bulk actions
 - 1.8.1.6.5. Delete users
 - 1.8.1.7. Managing access for user accounts
 - 1.8.1.7.1. Find and review users
 - 1.8.1.7.2. Update a user's roles
 - 1.8.1.7.3. Update a user's host group assignments
 - 1.8.1.7.3.1. Update host group assignments using bulk actions
 - 1.8.1.7.4. Update a user's cloud group assignments
 - 1.8.1.7.4.1. Update cloud group assignments using bulk actions
 - 1.8.1.7.5. Update a user's access scope assignments
 - 1.8.1.7.6. Reset user passwords
 - 1.8.1.7.6.1. Password requirements
 - 1.8.1.7.7. Reset Falcon MFA
 - 1.8.1.7.8. Generating a User details report
 - 1.8.2. Role Management
 - 1.8.2.1. Role Management
 - 1.8.2.2. Requirements
 - 1.8.2.3. Understanding Falcon role-based access control
 - 1.8.2.3.1. Multiple role assignments and access control
 - 1.8.2.4. Viewing role details
 - 1.8.2.5. Role permissions
 - 1.8.2.6. Role users and groups
 - 1.8.2.7. Managing custom roles
 - 1.8.2.7.1. Best practice: duplicate default roles
 - 1.8.2.7.2. Custom role examples
 - 1.8.2.7.2.1. Example: Admin role that can't create users
 - 1.8.2.7.2.2. Example: Admin role that can only create users
 - 1.8.2.7.3. Custom roles and Multi-CID environments
 - 1.8.2.7.4. Creating custom roles
 - 1.8.2.7.4.1. Recommended: create a custom role from a duplicate
 - 1.8.2.7.4.2. Create a custom role
 - 1.8.2.7.5. Edit custom role permissions
 - 1.8.2.7.6. Delete a custom role
 - 1.8.2.7.7. Best practice: Real Time Response roles and permissions
 - 1.8.3. Default Roles Reference
 - 1.8.3.1. Cross-subscription default roles
 - 1.8.3.2. Default roles by subscription
 - 1.8.3.2.1. Roles for Charlotte AI
 - 1.8.3.2.2. Roles for Cloud Security
 - 1.8.3.2.2.1. Deprecated Cloud Security roles
 - 1.8.3.2.3. Roles for Counter Adversary Operations
 - 1.8.3.2.3.1. Further reading
 - 1.8.3.2.3.1.1. For Falcon Sandbox
 - 1.8.3.2.3.1.2. For Falcon Intelligence broadly
 - 1.8.3.2.3.1.3. For Falcon MalQuery
 - 1.8.3.2.3.2. Roles for SampleStore
 - 1.8.3.2.4. Roles for Endpoint Detection and Response (EDR) scheduled searches
 - 1.8.3.2.5. Roles for Falcon Application Security Posture Management (ASPM)
 - 1.8.3.2.6. Roles for Falcon Complete
 - 1.8.3.2.6.1. Falcon Complete Hub
 - 1.8.3.2.6.2. Message Center
 - 1.8.3.2.7. Roles for Falcon Data Protection
 - 1.8.3.2.8. Roles for Falcon Discover for IoT
 - 1.8.3.2.9. Roles for Falcon Exposure Management
 - 1.8.3.2.9.1. Roles for asset management
 - 1.8.3.2.9.2. Roles for external surface attack management
 - 1.8.3.2.9.3. Roles for vulnerability management (Spotlight)

- 1.8.3.2.9.4. Roles for configuration assessment
- 1.8.3.2.10. Roles for Falcon FileVantage
- 1.8.3.2.11. Roles for Falcon Firewall Management
- 1.8.3.2.12. Roles for Falcon Flight Control
- 1.8.3.2.13. Roles for Falcon for IT
- 1.8.3.2.14. Roles for Falcon Forensics
- 1.8.3.2.15. Roles for Falcon Foundry
- 1.8.3.2.16. Roles for Falcon Identity Protection
- 1.8.3.2.17. Roles for Falcon Insight for Mobile
- 1.8.3.2.18. Roles for Falcon Insight Next-Gen SIEM
- 1.8.3.2.19. Roles for Falcon MalQuery
- 1.8.3.2.20. Roles for Falcon OverWatch
- 1.8.3.2.21. Roles for Falcon Prevent
- 1.8.3.2.22. Roles for scheduled reports
- 1.8.3.2.23. Roles for Falcon Shield
- 1.8.4. Access Scopes
 - 1.8.4.1. Overview
 - 1.8.4.2. Requirements
 - 1.8.4.3. Understanding access scopes
 - 1.8.4.3.1. How multiple access scopes work together
 - 1.8.4.3.2. How access scopes relate to host groups and cloud groups
 - 1.8.4.3.3. Granting all access scopes
 - 1.8.4.3.4. Limitations and considerations
 - 1.8.4.4. Setup
 - 1.8.4.5. Managing access scopes
 - 1.8.4.5.1. Create an access scope
 - 1.8.4.5.2. Edit an access scope
 - 1.8.4.5.3. Delete multiple access scopes at once
 - 1.8.4.5.4. Assign access scopes
 - 1.8.4.5.4.1. Assign access scopes to a single user
 - 1.8.4.5.5. Delete an access scope

1.9. Dashboards and Reports

- 1.9.1. Customizable Dashboards
 - 1.9.1.1. Overview
 - 1.9.1.1.1. Requirements
 - 1.9.1.1.2. Before you begin
 - 1.9.1.2. Understanding Falcon dashboards
 - 1.9.1.2.1. Info sources for dashboards
 - 1.9.1.2.2. Dashboard types: editing and sharing
 - 1.9.1.2.2.1. Preset dashboards
 - 1.9.1.2.2.1.1. Legacy dashboards
 - 1.9.1.2.2.2. Private dashboards
 - 1.9.1.2.2.3. Shared dashboards
 - 1.9.1.2.3. Single and multi source dashboards
 - 1.9.1.3. Setup
 - 1.9.1.4. Managing dashboards
 - 1.9.1.4.1. Getting to Dashboards
 - 1.9.1.4.2. Viewing dashboards
 - 1.9.1.4.2.1. Stay signed in when viewing dashboards
 - 1.9.1.4.3. Adding a dashboard
 - 1.9.1.4.3.1. Duplicating a dashboard
 - 1.9.1.4.3.2. Creating a single source dashboard
 - 1.9.1.4.3.3. Creating a multi source dashboard
 - 1.9.1.4.4. Editing a dashboard
 - 1.9.1.4.5. Managing widgets
 - 1.9.1.4.5.1. Moving and resizing a widget
 - 1.9.1.4.5.2. Adding a preset widget
 - 1.9.1.4.5.3. Creating or editing a custom widget
 - 1.9.1.4.5.4. Using time filters in dashboard widgets
 - 1.9.1.4.6. Sharing a dashboard
 - 1.9.1.4.7. Deleting a dashboard
- 1.9.2. Scheduled Reports
 - 1.9.2.1. Overview
 - 1.9.2.2. Requirements
 - 1.9.2.2.1. Default roles
 - 1.9.2.2.2. CrowdStrike clouds
 - 1.9.2.3. Understanding scheduled reporting
 - 1.9.2.4. Scheduled report settings
 - 1.9.2.4.1. Report data
 - 1.9.2.4.1.1. Data source
 - 1.9.2.4.1.2. Filters
 - 1.9.2.4.1.3. Dashboard types
 - 1.9.2.4.1.4. Data details
 - 1.9.2.4.2. Report details
 - 1.9.2.4.3. Report schedule
 - 1.9.2.4.3.1. Start date
 - 1.9.2.4.3.2. End date
 - 1.9.2.4.3.3. Frequency
 - 1.9.2.4.3.4. Time
 - 1.9.2.4.4. Notifications
 - 1.9.2.4.4.1. Notification delivery options
 - 1.9.2.4.4.1.1. Email
 - 1.9.2.4.4.1.1.1. Email attachments
 - 1.9.2.4.4.1.1.2. Calculating email attachment file size
 - 1.9.2.4.4.1.2. Slack
 - 1.9.2.4.4.1.3. PagerDuty
 - 1.9.2.4.4.1.4. Microsoft Teams
 - 1.9.2.4.4.1.5. Webhook
 - 1.9.2.5. Scheduled report limits
 - 1.9.2.6. Manage scheduled reports
 - 1.9.2.6.1. Access your scheduled reports
 - 1.9.2.6.2. View the list of scheduled reports
 - 1.9.2.6.2.1. View the report history
 - 1.9.2.6.3. Create a scheduled report
 - 1.9.2.6.3.1. About the report scheduler
 - 1.9.2.6.3.1.1. Schedule a new report
 - 1.9.2.6.4. Edit a scheduled report
 - 1.9.2.6.5. Run a scheduled report on demand
 - 1.9.2.6.5.1. To run a report on demand:
 - 1.9.2.6.6. Download a generated scheduled report
 - 1.9.2.6.7. Deactivate a scheduled report
 - 1.9.2.6.8. Take ownership of a scheduled report
 - 1.9.2.6.9. Delete a scheduled report
 - 1.9.2.6.10. Scheduled report notification configuration fields

1.10. Billing and Usage

- 1.10.1. Billing Dashboards for Usage and Licensing
 - 1.10.1.1. Billing Dashboards for Usage and Licensing
 - 1.10.1.2. Requirements
 - 1.10.1.3. Licensing
 - 1.10.1.4. Differences between single-CiD and multi-CiD environments
 - 1.10.1.5. View licensing with the Sensor subscription licenses dashboard
 - 1.10.1.6. View licensing with the Reserved and on-demand licenses dashboard
 - 1.10.1.7. View usage with the Sensor subscription licenses tab
 - 1.10.1.8. View usage with the Reserved and on-demand licenses tab
 - 1.10.1.9. View usage with the Sensor usage dashboard
 - 1.10.1.10. View POV usage and licensing data
- 1.10.2. Falcon Flex
 - 1.10.2.1. Overview
 - 1.10.2.2. Understanding your Flex commitment
 - 1.10.2.3. Dashboard
 - 1.10.2.3.1. Requirements
 - 1.10.2.3.2. Dashboard sections and widgets
 - 1.10.2.3.2.1. Flex Pool over time
 - 1.10.2.3.2.1.1. Flex simulator

Falcon Management

- 1.10.2.3.2.1.1.1. Export a Flex simulator report
- 1.10.2.3.2.2. Flex spend by product
- 1.10.2.3.2.3. Falcon bundles
- 1.10.2.3.2.4. Falcon modules
- 1.10.2.3.2.5. Available bundles and modules

1.11. Account Settings

- 1.11.1. IP Allowlist Management
 - 1.11.1.1. Overview
 - 1.11.1.2. Requirements
 - 1.11.1.3. Understanding the IP allowlist
 - 1.11.1.4. Managing IP allowlist groups
 - 1.11.1.4.1. Viewing your IP groups
 - 1.11.1.4.2. Creating an IP group
 - 1.11.1.4.3. Turning an IP group on or off
 - 1.11.1.4.4. Editing an IP group
 - 1.11.1.4.5. Deleting an IP group
 - 1.11.1.4.6. Viewing the IP allowlist audit log
- 1.11.2. SCIM Provisioning
 - 1.11.2.1. Overview
 - 1.11.2.2. Understanding SCIM
 - 1.11.2.2.1. Supported provisioning features
 - 1.11.2.2.2. Supported identity providers
 - 1.11.2.2.3. SCIM groups
 - 1.11.2.2.3.1. Role assignment
 - 1.11.2.2.4. SCIM base URL
 - 1.11.2.2.5. SCIM API key
 - 1.11.2.2.5.1. API key expiration
 - 1.11.2.2.5.2. API key expiration notifications
 - 1.11.2.2.6. Configuration mode
 - 1.11.2.2.6.1. Preview provisioned users and SCIM groups
 - 1.11.2.2.7. Falcon Flight Control support
 - 1.11.2.3. Set up SCIM provisioning
 - 1.11.2.3.1. Prerequisites
 - 1.11.2.3.2. Basic workflow
 - 1.11.2.3.3. Step 1: Set up SSO
 - 1.11.2.3.4. Step 2: Add the SCIM feature to your Falcon CID
 - 1.11.2.3.5. Step 3: Get your SCIM base URL and API key
 - 1.11.2.3.5.1. SCIM base URL
 - 1.11.2.3.5.2. SCIM API key
 - 1.11.2.3.6. Step 4: Configure SCIM in your IdP
 - 1.11.2.3.7. Step 5: Assign roles, host groups, and cloud groups to your provisioned SCIM groups
 - 1.11.2.3.8. Step 6: Preview provisioned users and SCIM groups
 - 1.11.2.3.9. Step 7: Transition from configuration mode to running SCIM in production
 - 1.11.2.4. Manage provisioned SCIM groups and users
 - 1.11.2.4.1. View provisioned SCIM groups in the Falcon console
 - 1.11.2.4.2. Manage SCIM group roles, host groups, and cloud groups
 - 1.11.2.4.2.1. Requirements
 - 1.11.2.4.2.2. Assign roles to a SCIM group
 - 1.11.2.4.2.3. View a SCIM group's assigned roles
 - 1.11.2.4.2.4. Assign host groups to a SCIM group
 - 1.11.2.4.2.5. Assign cloud groups to a SCIM group
 - 1.11.2.4.2.6. View a SCIM group's assigned host groups and cloud groups
 - 1.11.2.4.3. Add SCIM group users to Flight Control user groups
 - 1.11.2.4.4. Generate a new API key
 - 1.11.2.5. Set up SCIM provisioning with Okta
 - 1.11.2.5.1. Prerequisites
 - 1.11.2.5.2. Workflow process
 - 1.11.2.5.3. Create a SCIM app integration
 - 1.11.2.5.3.1. Add a SCIM 2.0 app to Okta
 - 1.11.2.5.4. Set up the SCIM connection
 - 1.11.2.5.4.1. Set up connection to an Okta SCIM app
 - 1.11.2.5.4.2. Set up connection to a SAML app
 - 1.11.2.5.5. Configure provisioning options
 - 1.11.2.5.6. Set user attribute mappings
 - 1.11.2.5.7. Sync users and groups to Falcon
 - 1.11.2.5.8. Management tips and integration limitations
 - 1.11.2.5.8.1. Okta user and group management
 - 1.11.2.5.8.2. Falcon user and group management
 - 1.11.2.6. Set up SCIM provisioning with Microsoft Entra ID
 - 1.11.2.6.1. Prerequisites
 - 1.11.2.6.2. Workflow process
 - 1.11.2.6.3. Create a SCIM app integration
 - 1.11.2.6.4. Connect your Falcon CID
 - 1.11.2.6.5. Set user and group attribute mappings
 - 1.11.2.6.6. Assign users and groups to your SCIM app integration
 - 1.11.2.6.7. Turn on provisioning
 - 1.11.2.6.8. Management tips and integration limitations
 - 1.11.2.6.8.1. Managing users and groups in Entra ID
 - 1.11.2.6.8.2. Managing users and groups in the Falcon console
 - 1.11.2.7. Set up SCIM provisioning with PingOne
 - 1.11.2.7.1. Prerequisites
 - 1.11.2.7.2. Workflow process
 - 1.11.2.7.3. Create a SCIM connection
 - 1.11.2.7.4. Enable the SCIM connection
 - 1.11.2.7.5. Configure an outbound group provisioning rule
 - 1.11.2.7.5.1. Set the target
 - 1.11.2.7.5.2. Define user filters
 - 1.11.2.7.5.3. Set user attribute mappings
 - 1.11.2.7.5.4. Select groups to provision
 - 1.11.2.7.6. Enable the rule
 - 1.11.2.7.7. Manage provisioned users and groups
 - 1.11.2.7.7.1. Manage users and groups in PingOne
 - 1.11.2.7.7.2. Manage users and groups in the Falcon console
 - 1.11.2.8. Set up SCIM provisioning with PingFederate
 - 1.11.2.8.1. Prerequisites
 - 1.11.2.8.2. Workflow process
 - 1.11.2.8.3. Create a SCIM connection
 - 1.11.2.8.4. Configure a provisioning channel
 - 1.11.2.8.5. Enable the SCIM connection
 - 1.11.2.8.6. Manage users and groups
 - 1.11.2.8.6.1. Manage users and groups in your provisioning source repository
 - 1.11.2.8.6.2. Manage users and groups in the Falcon console
 - 1.11.3. Single Sign-On (SSO) for Falcon
 - 1.11.3.1. Introduction
 - 1.11.3.2. Before you begin
 - 1.11.3.2.1. Supported identity providers
 - 1.11.3.2.2. Using SSO and Just-in-Time Provisioning
 - 1.11.3.2.3. User account management
 - 1.11.3.2.3.1. Manual user account management
 - 1.11.3.2.3.2. Automated user account setup with Just-in-Time provisioning
 - 1.11.3.2.3.2.1. Falcon Flight Control support
 - 1.11.3.2.3.2.2. Enabling Just-in-Time provisioning
 - 1.11.3.2.3.2.3. Disabling Just-in-Time provisioning
 - 1.11.3.2.4. Single sign-on terminology
 - 1.11.3.2.5. Certificate requirements
 - 1.11.3.3. Set up and use SSO
 - 1.11.3.3.1. Step 1: Configure your IdP
 - 1.11.3.3.1.1. Active Directory Federation Services (AD FS)
 - 1.11.3.3.1.1.1. Retrieving AD FS metadata
 - 1.11.3.3.1.2. Okta
 - 1.11.3.3.1.3. PingFederate
 - 1.11.3.3.1.3.1. 1. Assertion creation
 - 1.11.3.3.1.3.2. IdP adapter mapping
 - 1.11.3.3.1.3.3. 3. Protocol settings
 - 1.11.3.3.1.3.4. 4. SP Connection > Credentials

Falcon Management

- 1.11.3.3.1.4. PingOne
 - 1.11.3.3.1.5. Microsoft Entra ID
 - 1.11.3.3.2. Step 2: Contact us to configure Falcon SSO for your organization
 - 1.11.3.3.3. Step 3: Test logging in with SSO
 - 1.11.3.3.4. Step 4: Transition to SSO authentication
 - 1.11.3.4. Update your SSO configuration to use Just-in-Time provisioning
 - 1.11.3.5. Auditing
 - 1.11.3.6. Troubleshooting
 - 1.11.3.6.1. Issue: Can't log in with SSO
 - 1.11.4. FIDO Two-Factor (2FA) Authentication
 - 1.11.4.1. Overview
 - 1.11.4.1.1. Requirements
 - 1.11.4.1.2. Understanding FIDO two-factor authentication (2FA)
 - 1.11.4.2. Setup Overview
 - 1.11.4.2.1. Step 1: Develop a FIDO implementation plan
 - 1.11.4.2.2. Step 2: Register one or more FIDO devices
 - 1.11.4.2.3. Step 3: Enable FIDO for your CID
 - 1.11.4.2.4. Step 4: Inform your users
 - 1.11.4.2.5. Step 5: Test your FIDO setup by logging in
 - 1.11.4.3. Review users and their registered 2FA factors
 - 1.11.4.3.1. Export your user activity
 - 1.11.4.4. Recover lost two-factor authentication access
 - 1.11.5. Falcon Flight Control and Multi-CID Support
 - 1.11.5.1. Overview
 - 1.11.5.1.1. Understanding Falcon Flight Control vs. multi-CID accounts
 - 1.11.5.1.1.1. Falcon Flight Control partners
 - 1.11.5.1.1.2. Multi-CID customers
 - 1.11.5.1.2. Supported subscriptions
 - 1.11.5.2. Provisioning child CIDs using the Falcon console
 - 1.11.5.2.1. Requirements
 - 1.11.5.2.2. Add a new child CID
 - 1.11.5.2.2.1. Check provisioning status
 - 1.11.5.2.3. Multi-CID accounts
 - 1.11.5.3. Managing child CIDs
 - 1.11.5.3.1. Switch CIDs
 - 1.11.5.3.2. Add products to a child CID
 - 1.11.5.3.3. Remove products from a child CID
 - 1.11.5.3.4. Change a child CID's status
 - 1.11.5.3.5. View child CID provisioning details
 - 1.11.5.3.6. Track operations in the CID provisioning queue
 - 1.11.5.3.7. Review the provisioning audit log
 - 1.11.5.4. Provisioning child CIDs using the Partner Portal
 - 1.11.5.5. Managing policies
 - 1.11.5.5.1. Global policies (Falcon Flight Control)
 - 1.11.5.5.2. Local policies
 - 1.11.5.6. Managing detections
 - 1.11.5.6.1. Mobile detection exclusions
 - 1.11.5.7. Managing hosts
 - 1.11.5.7.1. Migrating hosts between CIDs
 - 1.11.5.7.1.1. Host migration requirements
 - 1.11.5.7.1.2. Understanding host migration
 - 1.11.5.7.1.2.1. Migration process overview
 - 1.11.5.7.1.2.2. Host migration CID domain requirements
 - 1.11.5.7.1.3. Create a host migration job
 - 1.11.5.7.1.4. Managing the host migration queue
 - 1.11.5.7.1.4.1. Migration job status
 - 1.11.5.7.1.4.2. Migration queue actions
 - 1.11.5.7.1.5. Managing a host migration job
 - 1.11.5.7.1.5.1. Host migration status
 - 1.11.5.7.1.5.2. Host migration job actions
 - 1.11.5.7.1.6. Troubleshooting host migrations
 - 1.11.5.7.1.6.1. Cloned host in destination CID for failed migrations
 - 1.11.5.7.2. Understanding host migration
 - 1.11.5.8. Managing scheduled reports
 - 1.11.5.9. Managing users
 - 1.11.5.9.1. Parent CID users
 - 1.11.5.9.2. Child CID users
 - 1.11.5.10. Managing workflows
 - 1.11.5.11. Visualizing your Flight Control environment
 - 1.11.5.11.1. Review your CID hierarchy
 - 1.11.5.11.1.1. Use Graph view
 - 1.11.5.11.1.1.1. View CID details
 - 1.11.5.11.1.1.2. Export and download
 - 1.11.5.11.1.2. Use Table view
 - 1.11.5.11.1.2.1. View CID details
 - 1.11.5.11.1.2.2. View a CID in the Graph tab
 - 1.11.5.11.1.2.3. Export and download data
- 1.11.5.12. Flight Control access management
 - 1.11.5.12.1. Understanding access management
 - 1.11.5.12.1.1. Default CID group
 - 1.11.5.12.1.2. Access management group limits
 - 1.11.5.12.1.3. Known issues
 - 1.11.5.12.2. Using access management
 - 1.11.5.12.3. Managing CID groups
 - 1.11.5.12.3.1. Accessing CID groups
 - 1.11.5.12.3.2. Viewing CID group details
 - 1.11.5.12.3.3. Creating a CID group
 - 1.11.5.12.3.4. Editing a CID group
 - 1.11.5.12.3.5. Deleting a CID group
 - 1.11.5.12.4. Managing user groups
 - 1.11.5.12.4.1. Accessing user groups
 - 1.11.5.12.4.2. Viewing user group details
 - 1.11.5.12.4.2.1. Users tab
 - 1.11.5.12.4.2.2. CID groups tab
 - 1.11.5.12.4.3. Creating a user group
 - 1.11.5.12.4.4. Assigning a CID group to a user group
 - 1.11.5.12.4.5. Assigning users to a user group
 - 1.11.5.12.4.5.1. Adding members to a user group from the User group details page:
 - 1.11.5.12.4.5.2. Assigning a user to a user group from the User details:
 - 1.11.5.12.4.6. Removing users from a user group
 - 1.11.5.12.4.6.1. Removing user group members from the User group details page:
 - 1.11.5.12.4.6.2. Removing a user from assigned user groups on the User details page:
 - 1.11.5.12.4.7. Removing CID groups from a user group
 - 1.11.5.12.4.8. Modify additional roles assigned to an associated CID group and user group
 - 1.11.5.12.4.9. Editing a user group name and description
 - 1.11.5.12.4.10. Deleting a user group
- 1.11.5.13. Generating an Access grant report
- 1.11.5.14. Viewing the Flight Control audit log
 - 1.11.5.14.1. Flight Control audit log events
- 1.11.5.15. APIs
 - 1.11.5.15.1. Detection APIs
 - 1.11.5.15.2. Restful APIs
 - 1.11.5.15.3. Streaming APIs
- 1.11.5.16. Falcon Data Replicator (FDR)

1.12. Assets

- 1.12.1. About Assets
 - 1.12.1.1. Understanding assets
 - 1.12.1.1.1. Asset protection
 - 1.12.1.1.2. Asset views
 - 1.12.1.2. Asset tasks
- 1.12.2. Asset Inventory
 - 1.12.2.1. Overview
 - 1.12.2.1.1. Requirements
 - 1.12.2.1.2. Before you begin
 - 1.12.2.2. Understanding custom tables

Falcon Management

- 1.12.2.2.1. Data sources for tables
- 1.12.2.2.2. Table types
- 1.12.2.3. Setup
- 1.12.2.4. View all assets
- 1.12.2.5. Manage custom tables
 - 1.12.2.5.1. View tables
 - 1.12.2.5.2. Add a table
 - 1.12.2.5.2.1. Duplicate a table
 - 1.12.2.5.2.2. Create a table
 - 1.12.2.5.2.2.1. Lock filter values
 - 1.12.2.5.3. Share a table
 - 1.12.2.5.4. Edit a table
 - 1.12.2.5.5. Delete a table
 - 1.12.2.5.6. Manage table groups
 - 1.12.2.5.6.1. Create table groups
 - 1.12.2.5.6.2. Add a table to a group
 - 1.12.2.5.6.3. Edit and delete table groups
 - 1.12.2.5.7. Export reports
 - 1.12.2.5.7.1. Quick exports
 - 1.12.2.5.7.2. Configure exports
 - 1.12.2.5.7.3. Download exported reports
 - 1.12.2.5.7.4. Configure export templates
 - 1.12.2.5.7.5. Edit export templates
 - 1.12.2.5.7.6. Delete export templates
- 1.12.3. Asset Criticality
 - 1.12.3.1. Asset criticality overview
 - 1.12.3.1.1. Requirements
 - 1.12.3.1.2. Understanding asset criticality
 - 1.12.3.1.2.1. Understanding criticality assignment
 - 1.12.3.1.2.2. Understanding Falcon recommended rules
 - 1.12.3.1.3. Asset criticality terminology
 - 1.12.3.1.4. Data refreshing
 - 1.12.3.2. Setup
 - 1.12.3.2.1. Set up criticality criteria
 - 1.12.3.2.2. Set up Falcon recommended rules
 - 1.12.3.2.2.1. Turn on Falcon recommended rules
 - 1.12.3.2.2.2. Turn off Falcon recommended rules
 - 1.12.3.3. Manage asset criticality
 - 1.12.3.3.1. Review criticality assignments
 - 1.12.3.3.2. Find assets by criticality
 - 1.12.3.3.3. Manually assign asset criticality levels
 - 1.12.3.3.4. Dynamically assign asset criticality levels
 - 1.12.3.3.4.1. Manage Falcon recommended criticality rules
 - 1.12.3.3.4.2. Find new Falcon recommended rules
 - 1.12.3.3.4.3. Create an asset criticality rule
 - 1.12.3.3.4.4. View asset criticality rule criteria
 - 1.12.3.3.4.5. Duplicate an asset criticality rule
 - 1.12.3.3.4.6. Edit an asset criticality rule
 - 1.12.3.3.4.7. Disable an asset criticality rule
 - 1.12.3.3.4.8. See all assets a rule applies to
 - 1.12.3.3.4.9. Delete an asset criticality rule
 - 1.12.3.3.5. Establishing rule precedence
 - 1.12.3.3.5.1. Change the precedence of asset criticality rules

Falcon Management

Use and administer Falcon overall. Manage users and roles, workflows, dashboards, reports, and more.

Learn about working with the Falcon console interface. Configure and manage core components and settings that are used to optimize features across the Falcon platform. View and manage information about your environment and account.

- Using the Falcon Console: Learn Falcon console basics including info about search and navigation, filtering, and profile settings.
- Falcon Notifications: Configure notifications to alert you about detections, policy changes, cloud security findings, and more.
- Dashboards and Reports: Create and manage customizable dashboards to help gain up-to-date, customized visibility into your Falcon environment. Create scheduled reports to get automatic, recurring updates of the data that matters most to you.
- User Management: Manage user accounts. Manage user access control, including roles, host group assignments, cloud group assignments, and Next-Gen SIEM access scopes. View Falcon console default role details and manage custom roles.
- Assets Overview and Inventory: Learn about assets, asset types, and protection options to understand where to find more info about monitoring assets and increasing security. Create custom tables for visibility into data about assets and cloud assets.
- Host and Host Group Management: View and manage hosts in your environment, monitor their health and status. View and manage host groups to facilitate protection policy assignments.
- Installation Tokens: Protect CIDs with installation tokens, preventing unauthorized hosts from being added.
- Detection Attribute Management: Customize which detection attributes appear for identity, endpoint, mobile, data protection, and unified detections.
- Falcon Browser Extension: Monitor files and data uploaded or downloaded in a browser. Prevent users from uploading files and clipboard data to websites and cloud applications. Configure Falcon browser extension settings.
- Falcon Flight Control and Multi-CID Support: For Falcon Flight Control or multi-CID account, leverage a parent/child hierarchy to efficiently manage policies, API access, and respond to detections.
- IP Allowlist Management: Help ensure your account is only accessed from specific networks by configuring your IP allowlist to restrict access to specific IP addresses.
- SCIM Provisioning: Automate user identity provisioning and management from your identity provider.
- Single Sign-On (SSO) for Falcon: Use SAML-based SSO to simplify user management and improve security controls.
- Billing Dashboards for Usage and Licensing: View dashboards to monitor sensor usage compared with purchased licenses across the environment.
- Falcon Flex: A flexible licensing model that allows you to buy CrowdStrike product licenses without committing to specific quantities.
- Falcon Status Dashboard: Review the current operational status of the Falcon platform based on reported issues and updated by the CrowdStrike team.

Falcon Console User Guide

Learn Falcon console basics including info about search and navigation, filtering, and profile settings.

Overview

This guide provides general information about the Falcon console, including access information, how to set up your preferences, and a high-level tour through the console's apps.

Supported browsers

The Falcon console supports the latest stable version of the following browsers:

- Google Chrome
- Microsoft Edge (Chromium)

Note: Because Falcon is browser-based, it's important to have the most up-to-date version of a supported browser installed. If you're experiencing issues accessing Falcon or using its features in a supported browser, make sure the browser is updated to the latest version.

Accessing the Falcon console

In a supported browser:

1. Go to your Falcon console URL. The URL depends on which cloud your organization uses. If you're not sure, refer to the initial setup instructions sent by CrowdStrike.

- US-1: <https://falcon.crowdstrike.com>
- US 2: <https://falcon.us-2.crowdstrike.com>
- US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com>
- EU-1: <https://falcon.eu-1.crowdstrike.com>

2. Enter your credentials on the login screen.

Tip: If you access one of the URLs in the previous step without using an SSO identity vendor tile, you see a Remember my email checkbox. Selecting the checkbox and logging in one time saves your email address locally in your browser. After that, whenever you have a link to Falcon, such as a link in an email to an alert or report, if you're using SSO but not logged in, you only need to click Continue to log in.

3. On the next screen, enter your 2FA token. The first time you sign in, you're prompted to set up a 2FA token. Common 2FA providers include Duo Mobile, winauth, JAuth, and GAAuth Authenticator.

For instructions about setting up roles and permissions, as well as instructions about resetting a password or 2FA, see [Users and Roles](#).

Note: The console session times out after 60 minutes with no activity. However, you can set dashboards to avoid timing out as explained in [Viewing dashboards](#), in the "Stay signed in when viewing dashboards" section.

Falcon console navigation

Navigation bar

Easily access the console menu, perform searches, switch customer IDs (CIDs), and more from the navigation bar.

Falcon Management



Navigation bar option	Description
	Open the console menu
	Navigation breadcrumb path of the current page
Bookmark this page	Add a bookmark for the current page
	Perform a search across the console
	Switch to another CID
Message center	Open the message center
Critical alerts and announcements	View notifications
Support	Access key pages like News, Falcon Documentation, and the CrowdStrike Customer Center
User profile	Go to your user profile or log out
Switch to light mode / Switch to dark mode	Switch between light and dark modes

CID switcher

The CID switcher displays the CID that your console session is currently logged in to. If you have roles in more than one CID, you can click your current CID to open a list of CIDs that you have access to.

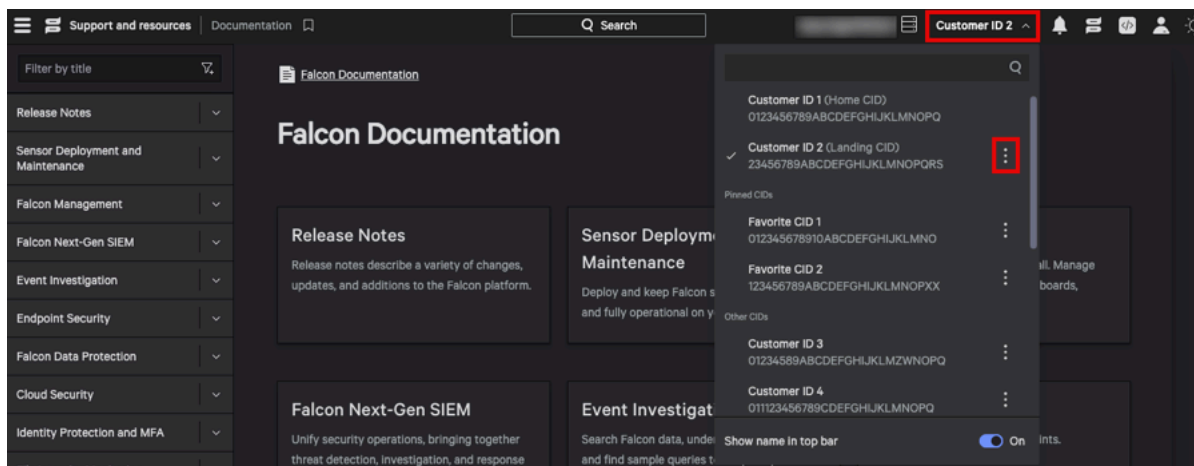


When you create a Falcon user account on a CID, that CID becomes your Home CID.

If you have access to multiple CIDs, you can use the CID switcher to perform these actions:

- Start typing a CID name or value in the CID switcher search bar to search for a particular CID.
- Click Open sub menu next to a CID and select one of these options:
 - Set as landing CID: Assign a CID as your default CID, which automatically opens whenever you log in to the console. If you lose access to your Landing CID, your Home CID becomes your default CID.
 - Pin CID: Add a CID to a group of favorite CIDs.
 - Unpin CID: Remove a CID from the Pinned CIDs group. It returns to the Other CIDs group.
 - Copy CID ID: Copy a CID to your clipboard.
 - Remove landing CID: Remove a CID as your default CID. It returns to the Other CIDs group.

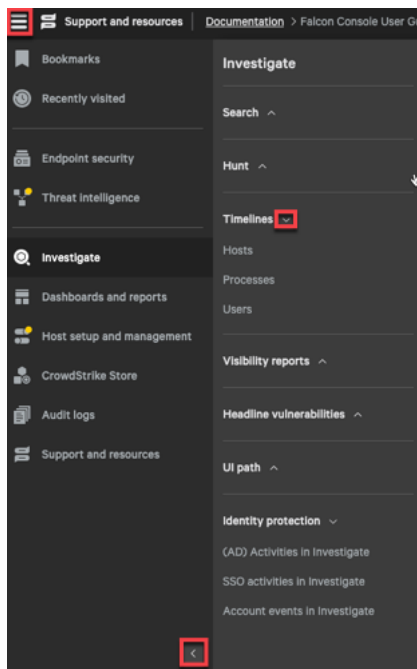
Falcon Management



Falcon console menu

The Falcon console menu is organized to help you find information and features quickly. To open the console menu, click Open menu  or use one of these keyboard shortcuts:

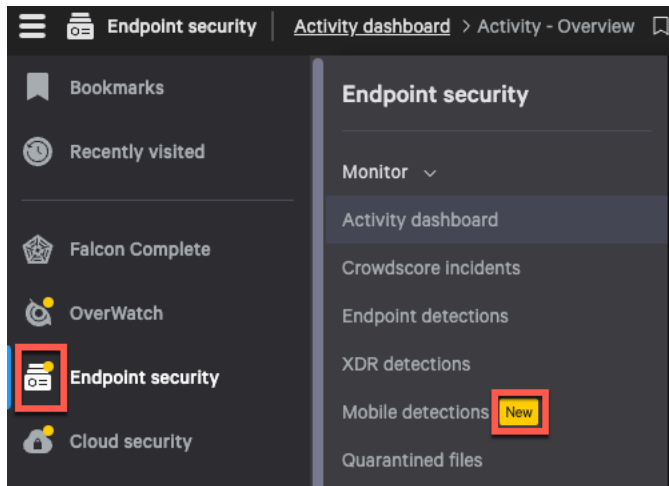
- Windows: Ctrl + /
- macOS: Command + /



Expand or collapse menu items to focus on what's important to you. Your display settings are remembered when you close the menu, such as which items are expanded or collapsed. When you open the menu again, the same view is presented.

Menu status flags

Menu items include status flags to draw attention to a specific area of the console. For example, if a page or feature is new. When a menu item includes a status flag, the parent menu item includes a badge to indicate the child menu item has a status flag.



Falcon console bookmarks

Build and manage your own list of bookmarks to easily navigate the Falcon console pages you visit most, including specific search results and pages with filters applied. Your bookmarks are available in the menu.

Note: Bookmarks are specific to both user and Customer ID (CID).

Create bookmarks

Create bookmarks for specific console pages, including any applied filters.

1. Go to the page you want to bookmark.

2. Click Add bookmark .

Tip: For best results, make sure pages load completely before bookmarking, especially pages that take a little longer to load like dashboards and pages with large tables.

3. In Save bookmark, update the Name, if desired.

Note: This field is populated differently in different areas of the console. For example, in Investigate, the Name field does not include the page title. However, the bookmark is saved for the exact page you are on and includes the precise filters you applied.

4. Click Save.

Your bookmark is available in the console menu.

Rename bookmarks

You can update the names of your bookmarks.

1. Go to the bookmarked page you want to rename.

2. Click Edit this bookmark .

3. In Edit bookmark, update the name.

4. Click Save.

Your bookmark is available in the menu with its new name.

Remove bookmarks

You can remove bookmarks you no longer need.

1. Go to the bookmarked page you want to remove.

2. Click Edit this bookmark .

3. In Edit bookmark, click Remove bookmark.

The removed bookmark no longer appears in the menu.

Remove all bookmarks

You can remove all of your bookmarks at one time through your user profile.

1. Go to your [User Profile](#) page.

2. Click User preferences in the User profile menu.

Falcon Management

3. Click **Reset preferences**.

Important: This removes all of your bookmarks and restores your user profile to default.

Central search

Using the new central search, you can see results from a number of key areas of the console and quickly go to more information. The central search returns the same results as doing a search on a supported Activity, Hosts, vulnerability management, or Intelligence page. It also returns results from the Docs and News areas of the Support app.

Use these keyboard shortcuts to start a search:

- Windows: Ctrl + K
- macOS: Command + K

Note: At this time, the central search does not support content in Investigate and asset management. Because these pages have a more robust search functionality, continue to search these pages separately.

Search input

Search input can be a unique identifier, like a hostname, hash, or file name. It can also be a word or topic to help find a doc or report. Areas handle search queries differently across the Falcon console, which can mean that some queries don't return all results you might expect. Use these guidelines to refine your search. As each area evolves how it handles search, those changes will improve results in the central search as well.

- Multiple-word queries return matches for each word instead of treating them as a phrase.
- Wildcards will work for searches of content on pages that support wildcard searches. We continue to work to bring all of the supported pages to parity.
- Adding quotes (" ") works for finding results in Adversaries and Reports. When you're interested in other result types, best practice at this time is to not use quotes.
- At this time, the search does not support logical operators (AND, OR, and NOT).

What is searched?

Where fields are not specified ("All"), the search covers all of the fields shown in the expanded list when you click in that page's filter field. Search looks at the available data, aligned with typical data retention. Expired data isn't searched. The search returns results from these pages:

- Endpoint security > Monitor > CrowdScore incidents (using host details, Name, Description, and Tags fields)
- Endpoint security > Monitor > Endpoint detections
- Endpoint security > Monitor > Quarantined files (using Filename and Hostname fields)
- FileVantage > File integrity monitoring > Changes
- Host setup and management > Manage endpoints > Host management
- Identity Protection > Monitor > Identity-based Detections (using detection id, detection name, assigned to name, destination application identifier, source endpoint IP address, user name)
- Identity Protection > Monitor > Users (using Primary Display Name and Secondary Name, SID)
- Identity Protection > Monitor > Endpoints (using Primary Display Name and Secondary Name)
- Exposure management > Vulnerability management > Vulnerabilities
- Support and resources > Support > Documentation
- Threat intelligence > Research > Adversaries
- Threat intelligence > Research > Reports and feeds
- Threat intelligence > Analyze > Sandbox
- Threat intelligence > Research > Indicators (domains, hashes, IP addresses)

Search suggestions

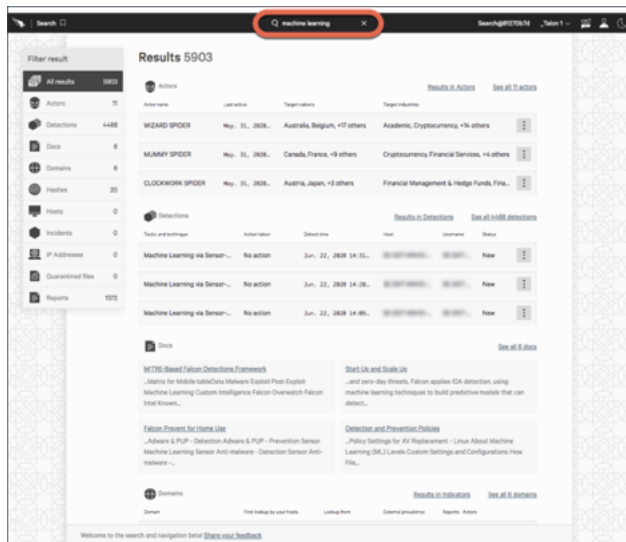
When you begin a search, the search field displays these search suggestions:

- Recent searches: Your last five search terms are saved and listed in your search suggestions so you can easily perform important repeated searches.
- Falcon console pages: When you enter a search term, search suggestions include Falcon console pages that match your term. For example, if you type Host, search suggestions are displayed that include all console pages that include Host in the title.

Search results

Search results are grouped by type. After each search, the main area of the page shows the Results preview, with a few results listed from each type that has matches.

Falcon Management



To see full search results of any type, use these options:

- In the Filter results legend on the left, click a type of search result to see all the results of that type.
- Within the Results preview:
 - Results in links take you to the full results for your search query on the relevant page of the console.
 - See all links show all of the results of that type.

Note: Each result type's page in this view has a discreet URL for easy sharing.

Click an individual search result within any area to go to that specific match. For example, a Docs result link takes you to that document, and a Detections result takes you to that detection's details.

If your organization has partner apps enabled through context enrichment in the CrowdStrike store, you might see IOC data from those apps in your search results. Results for partner app data include a link to the app for more details. See Data from partner apps.

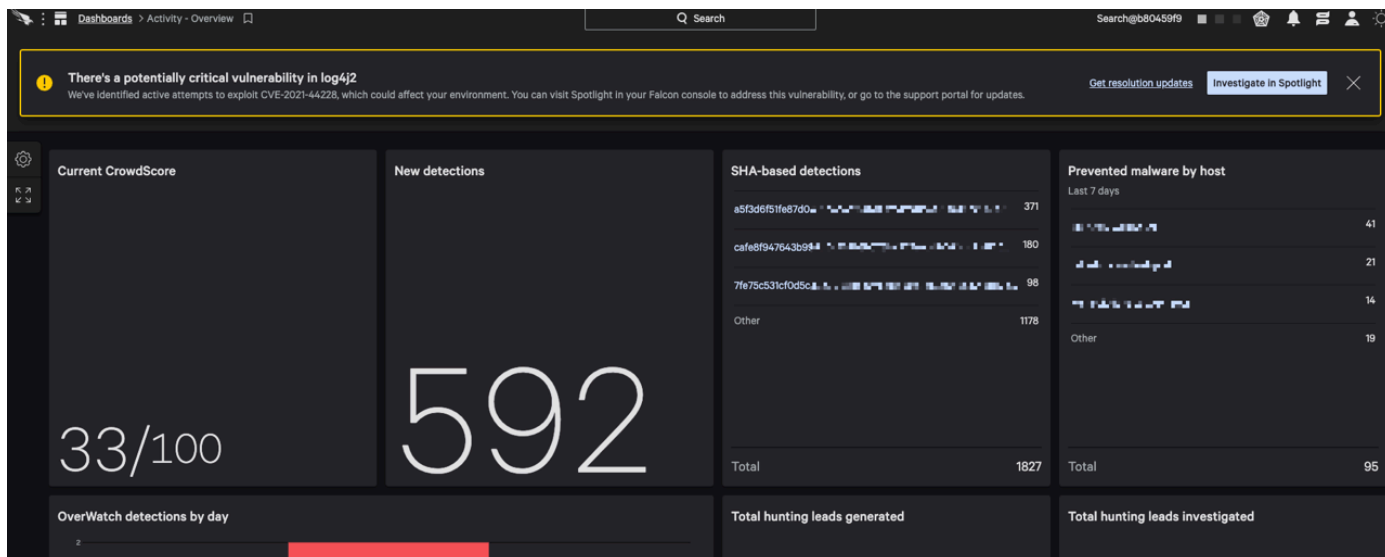
Falcon notifications

Stay informed of important news from CrowdStrike with console-wide critical alerts and announcements.

- Critical alerts
 - Critical alerts are near real-time notifications that raise your awareness about new major Common Vulnerabilities and Exposures (CVE) found around the globe.
 - These alerts can include links to the CVE and mitigation or remediation articles in the CrowdStrike Customer Center.
 - These alerts could also inform you of CrowdStrike's own security posture.
- Announcements
 - Announcements highlight upcoming events, product launches, and new features in the Falcon console.

You receive some messages because you're a CrowdStrike customer. You might receive other alerts based on your user role or subscription.

Note: Falcon notifications are important messages and are different from others you might see in the Falcon console.

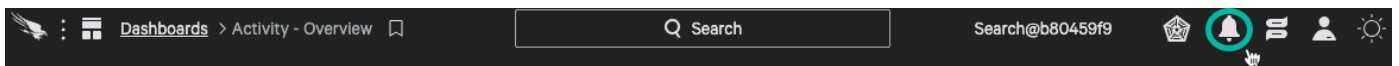


When you get an alert, you have these options:

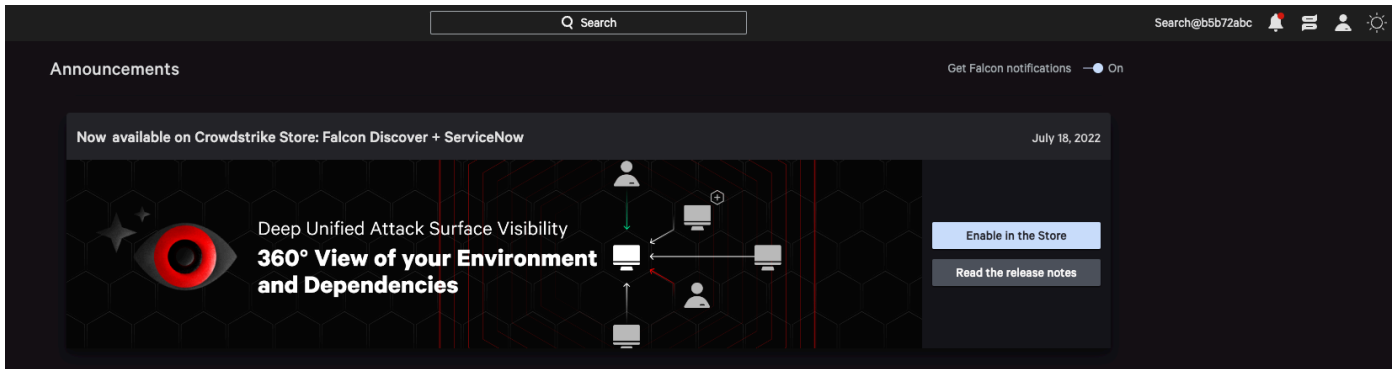
Falcon Management

- Follow the links in the alert to learn more and take action
- Dismiss the link and view it later using the Alerts and notifications page (Support and resources > Resources and tools > Notifications).

The notification bell is also a shortcut to this page. Select Critical alerts or Announcements.



On the Critical Alerts or Announcements pages, use the Receive Falcon notifications slider to turn off visual notifications and minimize interruptions from incoming alerts. All alert and announcement messages appear on these pages, regardless of this setting.



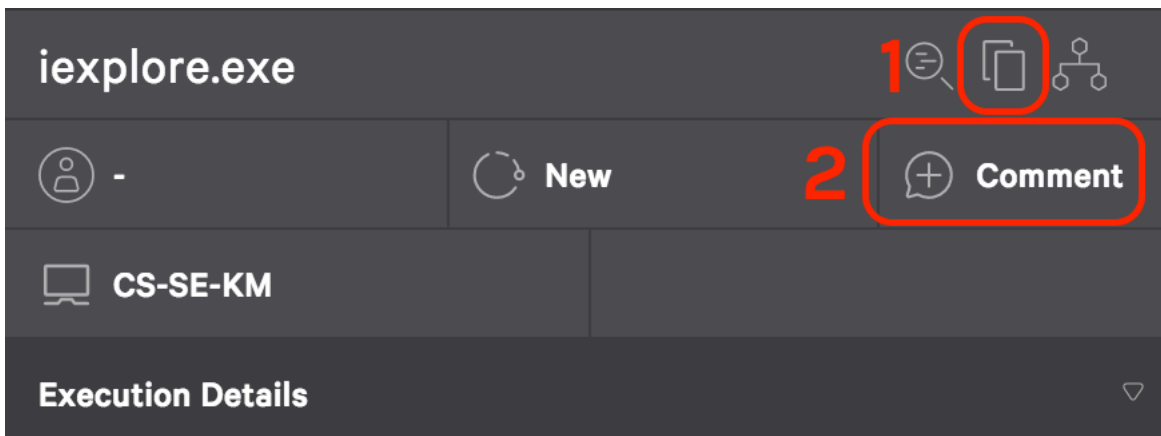
Overview of key features

This section covers key features that you will see across multiple apps in the Falcon console.

Comments and copy / paste

Throughout the console, there are different places to copy and paste data and add comments.

- Click the Copy button (1) to copy information from the screen or panel to your clipboard, simplifying the use of data between apps.
- Click the Comments button (2) to add comments that facilitate better communication between individuals and help track actions taken during triage.



ASSOCIATED BEHAVIOUR

Medium Severity Known Malware

Metasploit's meterpreter server may have been loaded into a process.

PREVALENCE

TBC

Customize columns

Throughout the console, you can add or remove columns in various tables by clicking the column selection button and checking/unchecking the desired fields. The example below is from the Hosts App.

Falcon Management

Hostname	Last Seen	OS Version	Model	Type	OU	Site Name
CS-SE-EZ64	Jul 25 @ 17:02	Windows 7	VMware Virtual ...	Workstation		
CS-SE-EZ64		Windows 7	VMware Virtual ...	Workstation		
CS-SE-EZ64	Jul 28 @ 06:36	Windows 7	VMware Virtual ...	Workstation		
DMARTINV...	Jul 20 @ 13:22	Windows 7	VMware Virtual ...	Workstation		Den2-Ops
IIS1		Windows Server...	VMware Virtual ...	Server		
vm0.local	Jul 18 @ 11:17	El Capitan (10.11)	VMware7,1			
WIN-RI99V...	Jul 27 @ 17:09	Windows 8.1	VMware Virtual ...	Workstation		

Select the columns you want to display in the table below:

- ☒ Hostname
- ☒ Last Seen
- ☒ OS Version
- ☒ Model
- ☒ Type
- ☒ OU
- ☒ Site Name
- ☒ Host ID
- ☒ Status

452ec3757c094... Normal

Data export

In many apps, you can export data on the screen to CSV or JSON format by clicking the export button (shown below):

50 Hashes found						
Action	List					
Never Block	323	Hashes-To-Block.txt @ August 9, 2016 7:19:35 PM +00:00				68
Always Block	104	putty_hashes.txt @ August 5, 2016 2:38:46 PM +00:00				34
No Action	36	qakhashes @ August 12, 2016 7:12:40 PM +00:00				4
Selected 0 of 463 Apply Policy						
Hash (SHA256)	File Name	Product...	Vendor	Version		
☐ 5e945c1d27c9ad77a2b63ae1...						
☐ 77dac064d0096dccc5e67c0...	m1c2.dll	Zip	Info-ZIP	5.5		
☐ 73c41e29e75e998a186e6fc74...					45 / 56	Always B...
☐ 240b43dfc2712d7d40312e76...					47 / 57	Always B...

Upload Hashes

Choose the type of file you want to download:

CSV

JSON

Filter bar

Use the filter bar on pages throughout the Falcon console to filter the data shown on that page.

Note: Many filter bar fields, but not all fields, support wildcards.

Click the filter bar to view a list of filters, click an individual filter, and then click a listed value or enter one yourself. Below is an example of the filter bar in Host Management that's filtering to show only hosts running Windows 10.

Host setup and management													
Host management													
Hosts													
Search all fields													
OS version = Windows 10													
Update													
Clear all													
One-click filters													
On													
158 Items													
Export													
Platform	OS version	OU	Site	Type	Network containment status	Tags							
Windows	Windows Server 2019			Workstation	Normal	N/A							
	Windows 10				Contained								
	Amazon Linux 2												
	Ubuntu 22.04												
	COS 113												
Hostname	Host ID	Last seen	First seen	Platform	OS version	Type	Local IP	External IP	MAC addr...	Sensor ve...	Host groups	Grouping ...	
		Oct. 4, 2024...	Oct. 4, 2024...	Windows	Windows 10	Workstation				717.18721.0			
		Oct. 4, 2024...	Oct. 4, 2024...	Windows	Windows 10	Workstation				717.18721.0			

Falcon Management

The filter bar also allows for multi-select of filters to quickly filter multiple values. This means that you can, for example, show Critical and High severity items from a list simultaneously.

The screenshot shows the 'Endpoint security' page with a search bar and a filter bar. The filter bar includes 'Severity: 2 applied', 'Time', 'Status', 'Tactic: Credential Access', 'Technique', 'Tags', 'Host', and 'Add/remove filters'. A dropdown menu is open for the 'Severity' filter, showing options: Critical (48), High (3,274), Medium (0), Low (0), and Informational (0). The 'Apply' button is highlighted. Below the filter bar, a table of detections is visible, with columns for 'Assigned to', 'Resolution', and 'Status'. The table shows several entries with 'Unassigned' resolution and 'New' status.

You can save a filter to access it more quickly in the future. Saved filters can be created, viewed, modified, and deleted by any Falcon console user with any role.

The screenshot shows the 'Host setup and management' page with a search bar and a filter bar. The filter bar includes 'OS version = Windows 10' and 'Update' button. A dropdown menu is open for the 'OS version' filter, showing options: Windows Server 2019 (565), Windows 10 (158), Amazon Linux 2 (111), Ubuntu 22.04 (57), and COS 113 (44). The 'Apply' button is highlighted. Below the filter bar, a table of hosts is visible, with columns for 'Last seen', 'First seen', 'Platform', 'OS version', 'Type', 'Local IP', 'External IP', 'MAC addr...', 'Sensor ve...', 'Host groups', and 'Grouping...'. The table shows several entries with 'Windows' platform and 'Windows 10' OS version.

Data from partner apps

If your organization has partner apps enabled through context enrichment in the CrowdStrike store, you might see data from that app in the Falcon console. Partner app data appears in central search results and on incident pages in relation to these types of IOC: hashes, domains, and IP addresses. For more info, see Endpoint Incident Monitoring.

The screenshot shows the 'Falcon Endpoint' page with a search bar and a filter bar. The filter bar includes 'Falcon Intel', 'DomainTools', 'OPSWAT', 'RiskIQ', and 'Sixgill'. A dropdown menu is open for the 'Falcon Endpoint' filter, showing options: External prevalence (Common), Internal prevalence (Common), Last seen (Oct. 21, 2020 08:48:26), # of hosts (87), and # of detections (0). The 'Apply' button is highlighted. Below the filter bar, a timeline chart is visible, showing data points from Feb. 20, 2018 16:56:54 to Oct. 21, 2020 08:48:26.

When data from a partner app is shown in a result, click the See more on [partner app] link to go to the app and see more details.

When viewing IOC data in search results or on an incident page, click Manage Apps or Add Apps to go to the CrowdStrike store and manage your partner app integrations.

When you go to the CrowdStrike store from IOC data in the Falcon console, the list of available apps is filtered by IOC type. For example, if you click Manage Apps or Add Apps from the Executable Hash area of an incident page, you are shown available partner apps for hash data in the CrowdStrike Store. See CrowdStrike Store documentation.

Profile settings

Go to your [User Profile](#) page to change or view the following items.

The Profile tab provides this info:

- Email
- First name and last name
- Home CID and current CID
- The privacy policy

Use the Account security tab to complete these tasks:

Falcon Management

- Change password
- Set up multi-factor authentication
- Get a verification code to verify your identity with Support

Use the User preferences tab to complete these tasks:

- Set timezone, date format, or locale

This timezone is used for detection information. By default, the Falcon console displays times in local browser time for all detections and other components that use a time—with the exception of Event Search data, which uses UTC.

You can change the display language of the Falcon console. The Falcon console is fully available in English. We are continuously adding support for Japanese throughout the Falcon console.

- Show or hide your search history in the search suggestions of the Falcon console central search
- Enable or disable to set your preferred host management page experience
- Reset your profile to the default

Falcon Status Dashboard

Review the current operational status of the Falcon platform based on reported issues and updated by the CrowdStrike team.

Overview

In the Falcon Status dashboard, review the current operational status of the Falcon platform based on reported issues and updated by the CrowdStrike team.

- See the status of the CrowdStrike features you're subscribed to and features available to all CrowdStrike customers.
- View the context of a status, like a status summary or a link to a [CrowdStrike tech alert](#).
- See Timestamps, so you know the duration of a status and when it's resolved.

This dashboard is available to all CrowdStrike customers with a subscription. No setup is required.

Understand the dashboard

To view the dashboard, go to Support and resources > Resources and tools > Falcon status in the Falcon console.

Support and resources | Falcon status

Search

Falcon Status

The current operational status of the Falcon platform, updated by the CrowdStrike team

Features 25 items

Status

All

Tech Alerts

Feature name	Status	Details	Actions
Authentication and SSO	✓ Available	--	⋮
Charlotte AI	✓ Available	--	⋮
Cloud Security	✓ Available	--	⋮
CrowdStrike Store	✓ Available	--	⋮
Customer API	✓ Available	--	⋮
Data protection	✓ Available	--	⋮
Detections	✓ Available	--	⋮

Feature name

The Feature name column lists features you're subscribed to, including these features available to all CrowdStrike customers regardless of subscription:

- Authentication and SSO
- Falcon Console/UI
- Customer API
- Fusion SOAR
- Host Management
- Policy
- Sensor

To organize the dashboard view by feature name, click the arrows  in the Feature name column header to sort by ascending or descending alphabetical order.

Falcon Management

Status

The Status column shows the current operational status of the listed features.

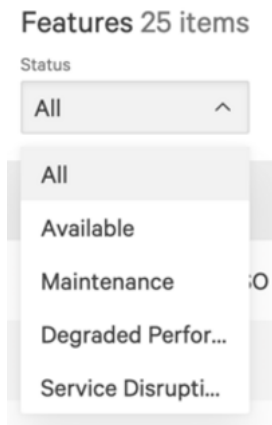
Note: Status is not customized for individual environments and may not reflect issues reported in specific pod or cluster environments.

Status options:

- Available: Operating normally with no known issue.
 - Maintenance: Service may be unavailable or partially impacted during maintenance.
 - Degraded Performance: Service delayed or has limited functionality.
 - Service Disruption: Service is unavailable or unable to provide primary functionality.
- Note: The LogScale Console and Investigate/Search feature names only show the maintenance and available status.

To organize the dashboard view by status, click the arrows  in the Status column header to sort by ascending or descending alphabetical order.

To view features in a specific operational status, filter by a status in the Status dropdown menu. By default, statuses are filtered by All.



Details

The Details column provides additional info about feature status. For example, the CrowdStrike team may link to the most recent tech alert available in the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, go to the [CrowdStrike Government Customer Center](#).

Tech Alerts

To view the most recent tech alert for a status, click the tech alert link in Details. Once feature status is set to Available again, the link to the tech alert is removed after 24 hours, by default.

Note: This dashboard only provides the most recent tech alert for a status. A status may have multiple tech alerts. From the main view of the dashboard, click Tech Alerts to see the full list of tech alerts. You can also see the Latest Updates section in the tech alert, if available.

Actions

In the Actions column, click the Open menu  and click Open details panel to see additional info related to status:

- Status: The current operational status of the Falcon feature you're subscribed to.
- Summary: A summary of the current status.
- Started on: The date and a timestamp when the current status started.
- Duration: The duration of the current status, including elapsed time, in timestamp format, and days.
- Details: Additional info about the current status, which may include a link to a tech alert, if available.
- Resolved: Date and timestamp of a resolved status. This remains until the tech alert is removed from Details.

To close the details panel, click Close .

Host and Host Group Management

View info about, delete, and network contain your hosts. Plan, create, and assign hosts to host groups.

Requirements

Subscription: Host management is applicable to any subscription.

Default roles: Management of host groups is handled by cross-subscription default roles. For more info, see [Cross-subscription default roles](#).

The Falcon Administrator role is required for hiding and deleting hosts.

These cross-subscription default roles can see host management and manage host groups:

Falcon Management

- Falcon Administrator
- Endpoint Manager

These cross-subscription default roles can see host management but are unable to manage host groups:

- Prevention Policy Manager
- Falcon Analyst
- Help Desk Analyst

Note: This role allows users to see host information, but not related user information. To see user information in host management, a role that grants access to user information must also be assigned.

Managing Hosts

View important info about your hosts and manage them using actions such as adding or removing tags, updating containment status, and enabling or disabling detections.

Viewing host overview info

The [Hosts Overview](#) dashboard displays high-level info about your hosts such as the number of hosts per host type, the number of hosts that are online or offline, the number of hosts on each platform and operating system, the number of hosts using each applicable sensor version, the number of hosts on each applicable domain, and the number of hosts with specific policies enabled. The dashboard also displays high-level pod info for cloud containers secured with Falcon Container sensor for Linux.

Navigating the Host Management page

On the [Host Management](#) page, view information about each host including OS, host type, the prevention policy applied to the host, and a host's containment status and sensor version.

From this page, you can see which prevention policy is applied to a host. The Prevention Policy column can have the following values:

- "No Policy" - Used if the host recently had a Falcon sensor installed on it, and either the cloud has not yet evaluated which policy is appropriate or the host is no longer active.

Note: All ChromeOS hosts will have the "No Policy" status appear for all policies.

- "{Policy Name}" & "{Applied Date}" - Name of the policy that has been pushed down to the host and the date and time at which the host received the policy.
- "{Policy Name}" & "Changes pending" - Name of the policy that will be pushed down to the host.
- "Policy Deleted" & "Changes pending" - The host has a policy that has been deleted and the cloud has yet to determine which new policy the sensor should receive. During this transitional period, the host will continue to use the policy that was previously applied to it as it waits to receive the new policy from the cloud.

Click a policy name to view and edit that policy on the Prevention Policies page.

Tip: See [Falcon Insight for ChromeOS](#) to learn more about ChromeOS host management.

Find a host

The [Host Management](#) page lets you filter, search, and customize the columns you see to help you find and manage your hosts.

Use the filter bar at the top to search for a specific host, or click the default filters to view a more targeted list.

Important: These filter bar attributes are case-sensitive:

- Architecture
- CPUID
- Cloud Service Provider
- Cloud service zone/group
- Domain
- Email
- Tags
- Kubernetes Cluster Git Version
- Kubernetes Cluster Id
- Kubernetes Cluster Version
- Manufacturer
- Model
- RFM
- Serial Number

To choose the columns that appear on the Host Management table, click the configure table columns icon , and then select the desired columns.

View a host's summary panel

To open the summary panel for any host, click a host name in the list.

Note: Information that displays on the host summary panel varies by Falcon product subscription and your assigned user roles.

Host status information and quick links to perform various actions are available at the top of the panel:

Falcon Management

- See the host's current online status
 - Online (blue): The host was seen recently, and we are confident it's currently online.
 - Offline (gray): The host has not been seen for some time, and we are confident it's currently offline.
 - Unknown (amber): The host has not been seen recently, and we are not confident about its current state.
- Connect to the host and perform real time response actions
- Disable or re-enable detections on the host
- View and change the host's containment state
- Delete the host
- Reveal the host maintenance token that's required to uninstall the sensor

Note: You can view maintenance tokens only for hosts in your current CID.

Note: Real time response actions are not supported for ChromeOS hosts.

Other host details are organized in focused sections for quick visibility and access to resources and settings. See host info, user info, policy info, cloud service info, and more. Sections that are not applicable to the host or that contain no data are grayed out.

Host timeline

With the host timeline, see a history of host states and events, such as when a host was online, if a host was contained and for how long, or when a host's sensor was provisioned. Leverage historical data to address common troubleshooting issues and gain insight into end user and Falcon administrator behavior.

To open the timeline for a host, on the Host Management page:

- In the Host Management table, click the Actions menu for a host and select Host timeline
- From the Host information panel, click Actions > Host timeline

A link to a host's timeline is also available in other areas of the Falcon console where you can get to more info about a specific host, such as search results.



Note: During periods of high activity, such as during sensor updates, the host timeline might stop processing the online state. During this time, an online host continues to have an accurate Host status value on the Host Management page, but the Online state doesn't appear in the Host timeline.

Host states and events

The host timeline includes these sections:

- States: This area shows the duration of time a host is in each state, such as online, contained, or hidden.
- Events: This area shows singular events such as First seen, or an event that prompts a state change, such as a Containment request.

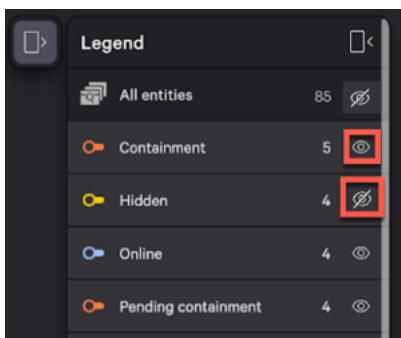
Click a state, an event, or a group of events in the timeline to open the Selection Summary panel with more information, such as start and end times and attributes.

Modifying the host timeline

You can modify the host timeline to narrow or broaden the scope of states and events in these ways:

Falcon Management

- Apply state or event filters: In the Legend, click the show or hide icons for a specific state or event layer. Hidden states and events don't appear in the timeline.



- Modify the time frame: Select any time frame to broaden or narrow the duration shown in the timeline. The host timeline shows information for the previous 7 days by default. You can select a time frame up to the previous 45 days.
- Zoom in to a smaller area of the existing time frame: Click and drag the area above the timeline to zoom in to a smaller section. This area above the timeline displays dots to indicate there are states or events to zoom in on.



- Expand events: By default, the Events section of the timeline shows all events in the same lane, or vertical space on the horizontal axis, grouping events that happen together and indicating how many events are in the group. Click Expand to expand the events section of the timeline so each event type has a dedicated horizontal space. This is helpful to see more info when there are event clusters.

Events list

Click the Events List tab to view host events in a table. By default, the most recent events are listed first. You can sort, filter, and export the table of events.

Export host data

Export host data to CSV or JSON format.

Exported host data includes only hosts that meet current filter criteria, and can contain up to one million items. This data includes all selected host columns. For more info about configuring columns, see [Configure exports](#). Up to five exports can be requested at one time per user.

Quick exports

Export a CSV file of the info as you see it in the console, or export from a saved template.

1. Click Export.
2. Select a quick export option:
 - Choose CSV of current selection to export the table as a CSV file.
 - Choose a saved export template.

Configure exports

Configure exactly which data you want to see in an export.

1. Click Export.
2. Select New export or template.
3. Select CSV or JSON.
4. In the Available data section, select the columns you want to include in your exported report. By default, the Selected data section includes the data visible in the current table.

Note: The CID and Host ID columns can't be excluded from JSON exports of the Hosts and Hidden hosts table.
5. In the Selected data section, drag the data to reorder it in your export.

Falcon Management

6. Click Export.

Download export reports

View and download the 10 most recently run exports.

1. Click Export.
2. Select Completed exports. The Completed exports section shows the number of exported reports that are ready to download.
3. Click Download  for the report you want. The export report downloads to your device's default downloads folder.
Tip: If your download is too big, apply more filters.

Files are available for 72 hours after initially requesting the download.

Configure export templates

Save an export as a template to reuse within your environment. Export templates are shared within an environment across users. Environments can have a maximum of 10 saved templates.

1. Click Export.
2. Select New export or template.
3. Click Save as template for future use to reuse the configuration as a template.
4. Enter a name.
5. Select CSV or JSON.
6. From the Available data section, choose the data you want to see in your export.
7. In the Selected data column, drag the columns to reorder them in your export. By default, the Selected data column includes the columns visible in the current table.
8. Click either Save and export or Save without exporting.

Edit export templates

Edit export templates to match your environment's needs.

1. Click Export.
2. Select Saved templates.
3. Click Edit  to edit a template.

Delete export templates

Delete export templates that no longer meet your environment's needs.

1. Click Export.
2. Select Saved templates.
3. Click Delete  to delete a template.

View content update states

View content package states for hosts in your environment, including current policy settings and the timestamp for when a specific host was last updated with content for each category.

For more info about configuring content update policies, see Content Update Policies.

1. Go to Host setup and management > Manage endpoints > Content update states .
2. For each host, view this content update info:
 - o Content update policy: View the currently-applied policy for the host and the timestamp of when it was applied.
 - o Last updated: View the timestamp of the last content update the host received for each category.
Important: This timestamp indicates when a specific host received a content update. Hosts receive content updates as part of a gradual rollout in each delivery phase. You can view the current global deployment status of a content package update, including when a specific phase was completed across all hosts using the Content quality dashboard. Go to Dashboards and reports > Dashboards > Content quality dashboard . See View content package updates deployment status.
 - o Policy setting: View the current delivery phase policy setting, such as GA or Pause, for each content update category. The policy setting columns also show whether a version has been pinned for a content update category. Deployment settings are defined in the configuration of the content update policy that is currently applied to the host.
 - o Override status: View whether or not the host's currently-applied policy has an override configured.
3. Use standard host management filters to view a subset of hosts that meet content update filter criteria, such as hosts that received content updates for Sensor Operations within the last 24 hours.

Managing inactive and duplicate hosts

Clean up inactive or duplicate hosts by hiding or deleting them from the console. This is helpful when managing inactive, duplicate, or ephemeral hosts. You can manually hide hosts or you can create host retention policies to automatically hide or delete inactive hosts. If you don't hide hosts or apply a host retention policy, inactive hosts are deleted from the console after the system default inactivity period of 45 days.

Note: The Falcon Administrator role is required for hiding and deleting hosts.

An inactive host is a host that has a status of Offline. A host's duration of inactivity is identified by their Last seen value.

Duplicate hosts typically appear when sensor installations fail. After another installation attempt that is successful, the Hostname and Serial number values stay the same, but the Falcon sensor gets a new Host ID value. You can hide or delete the previous records so only the most recent, active hosts appear in the console.

Falcon Management

Understanding host hide and delete actions

You can clean up the Falcon console by hiding or deleting hosts. When you hide or delete a host, the sensor is not deactivated or uninstalled. Detections that were generated before the host was hidden or deleted remain visible in the console for 90 days. Otherwise, these differences apply to the hide and delete actions:

- **Hide:** Hiding a host is useful if you want to reduce the clutter in the console but leave the option to restore the host later. When a host is hidden it is moved to the Hidden hosts page and removed from all other pages of the Falcon console. You can manually hide hosts or you can use the auto-hide option in a host retention policy. See [Manually hide a host](#) and [Host retention policies](#).
Important: You can't restore a hidden mobile host. See [Hiding mobile hosts](#).
- **Delete:** Deleting a host is useful if you are confident the host is no longer relevant and you want to remove it from the console without the option to restore it later. When a host is deleted it is permanently removed from all pages of the Falcon console. You can't manually delete a host. Hosts are only deleted according to the settings of an applied host retention policy or the system default of 45 days of inactivity. See [Host retention policies](#).

Additionally, if a host comes back online, the behavior is different depending on whether it was hidden or deleted:

- **Hide:** If a hidden host comes online, it remains hidden until you restore it to the console manually or by using the Auto-restore active hidden hosts setting. See [Restore a host](#). Hidden hosts that are online continue to send events to the CrowdStrike cloud but those events aren't reported in the console and they don't trigger workflows, appear in the Event Streams API, or trigger detection emails. Prevention settings continue as configured and hidden online hosts continue to receive policy updates.
- **Delete:** If a deleted host comes online, it is automatically restored. If a host was hidden before being deleted, it is not restored to the Hidden hosts page, but completely restored to the console. Deleted hosts that are restored have a new First seen date and are restored to the appropriate containment status based on the state of the sensor. Deleted hosts that are restored lose any previously-assigned Falcon grouping tags but retain sensor grouping tags. This means they resume host group assignments, after a delay, unless the host group assignments use Falcon grouping tags. For more info about tags, see [Group hosts using tags](#).

Note: Hiding a ChromeOS host is similar to hiding hosts on Windows, Mac, and Linux. However, ChromeOS machines are enrolled through the Google Admin console and do not have a sensor installed. See [Falcon Insight for ChromeOS](#).

Hiding mobile hosts

Use caution if you hide mobile hosts. When you hide a mobile host:

- The host is permanently removed from the console. It doesn't remain active or appear on the Hidden hosts page and can't be restored. If a mobile host is accidentally hidden, a new invite needs to be sent to the associated user so they can re-enroll.
- All data associated with the CrowdStrike Falcon app is removed.
- If there was a per-app VPN profile applied to the unsupervised iOS device, it remains in effect - cutting off data flow for the apps that were monitored by Falcon. You might need to apply a different profile to the device.

For more info about how to hide a host, see [Manually hide a host](#).

Host retention policies

Use host retention policies to automatically hide or delete inactive hosts from the Falcon console after a specified period of inactivity. An inactive host is a host that has a status of Offline.

Important: You can only create policies for Windows, Mac, Linux, ChromeOS, and Kubernetes (K8) hosts. Host retention policies are not applied to mobile hosts, iOS and Android.

Tip: For info about how policies work, including host group assignment and policy precedence, see [Policies in Falcon](#).

Host retention policy assignment and precedence

Host retention policies function the same way as prevention policies. They are assigned to hosts through host group membership and if more than one policy is assigned to a host, the policy with the highest precedence is applied. If a host isn't assigned a host retention policy, the default policy is applied.

A retention policy can only be applied to hosts that connect to the CrowdStrike cloud after the policy is assigned. Hosts that are offline when the policy is assigned, and remain offline, do not get assigned the retention policy and are deleted according to either a previously-applied policy or the default policy of 45 days of inactivity.

More info:

- For more info about updating the settings of the default host retention policy, see [Manage settings for a host retention policy](#).
- For more info about setting policy precedence, see [Manage host retention policy precedence](#).

Important: If the host retention policy applied to a host through policy precedence doesn't have the Auto-delete hosts setting enabled, the host is automatically deleted from the console after the system default of 45 days of inactivity. This happens regardless of the Auto-delete hosts setting of any other host retention policy assigned to the host, including the default policy, because the Falcon platform adheres to the settings of the applied policy only. For more info about the Auto-delete hosts setting, see [Manage settings for a host retention policy](#).

Create a host retention policy

1. Go to [Host setup and management](#) > [Manage endpoints](#) > [Host management](#) , then click the Host retention policies tab.
2. Click [Create policy](#).
3. In the [Create policy](#) dialog, specify a policy name and optional description, and then click [Create policy](#).

The host retention policy details page opens.

4. You must assign the policy to one or more host groups for it to be applied to hosts:
 - a. On the [Assigned host groups](#) tab, click [Assign host groups to policy](#).
 - b. In the [Assign host groups to policy](#) dialog, select the desired host groups, and then click [Assign groups](#).
5. On the [Settings](#) tab, specify these settings:

Falcon Management

- o Auto-hide hosts: Enable this setting to automatically hide inactive hosts when they have reached a specified duration of inactivity.
 - o Auto-hide inactivity period: If the Auto-hide hosts setting is enabled, select the duration of inactivity. Hosts that have been inactive for this duration are automatically hidden from the Falcon console and moved to the Hidden hosts page.
 - o Auto-delete hosts: Enable this setting to automatically delete inactive hosts when they have reached a specified duration of inactivity.
 - o Auto-delete inactivity period: If the Auto-delete hosts setting is enabled, select the duration of inactivity. Hosts that have been inactive for this duration are automatically deleted from the Falcon console.
6. Click Save.

For info about the difference between hiding and deleting a host, see [Understanding host hide and delete actions](#).

Duplicate a host retention policy

1. Go to [Host setup and management > Manage endpoints > Host management](#) , then click the [Host retention policies](#) tab.
2. Click the name of the retention policy you want to duplicate.

The host retention policy details page opens.
3. Click [Duplicate policy](#).
4. In the Duplicate policy dialog, specify a policy name, optional description, and whether to assign the same host groups to the new policy, and then click [Duplicate](#).
5. Optional. Update the assigned host groups:
 - a. On the [Assigned host groups](#) tab, click [Assign host groups to policy](#).
 - b. In the [Assign host groups to policy](#) dialog, select the desired host groups, and then click [Assign groups](#).
6. Optional. On the [Settings](#) tab, update these settings:

- o Auto-hide hosts: Enable this setting to automatically hide inactive hosts when they have reached a specified duration of inactivity.
- o Auto-hide inactivity period: If the Auto-hide hosts setting is enabled, select the duration of inactivity. Hosts that have been inactive for this duration are automatically hidden from the Falcon console and moved to the Hidden hosts page.
- o Auto-delete hosts: Enable this setting to automatically delete inactive hosts when they have reached a specified duration of inactivity.
- o Auto-delete inactivity period: If the Auto-delete hosts setting is enabled, select the duration of inactivity. Hosts that have been inactive for this duration are automatically deleted from the Falcon console.

7. Click Save.

For info about the difference between hiding and deleting a host, see [Understanding host hide and delete actions](#).

Manage settings for a host retention policy

To manage the settings for an existing host retention policy, including the default policy:

1. Go to [Host setup and management > Manage endpoints > Host management](#) , then click the [Host retention policies](#) tab.
2. Click the name of the retention policy you want to manage.

The host retention policy details page opens.
3. On the host retention policy details page, manage these settings:
 - o [Edit the name and description of the policy](#)
 - o [Disable or enable a policy](#)
4. To update the assigned host groups:
 - a. On the [Assigned host groups](#) tab, click [Assign host groups to policy](#).
 - b. In the [Assign host groups to policy](#) dialog, select the desired host groups, and then click [Assign groups](#).
5. To update the auto-hide and auto-delete settings, click the [Settings](#) tab, update this info, and then click [Save](#):
 - o Auto-hide hosts: Enable this setting to automatically hide inactive hosts when they have reached a specified duration of inactivity.
 - o Auto-hide inactivity period: If the Auto-hide hosts setting is enabled, select the duration of inactivity. Hosts that have been inactive for this duration are automatically hidden from the Falcon console and moved to the Hidden hosts page.
 - o Auto-delete hosts: Enable this setting to automatically delete inactive hosts when they have reached a specified duration of inactivity.
 - o Auto-delete inactivity period: If the Auto-delete hosts setting is enabled, select the duration of inactivity. Hosts that have been inactive for this duration are automatically deleted from the Falcon console.

For info about the difference between hiding and deleting a host, see [Understanding host hide and delete actions](#).

Manage host retention policy precedence

If a host is assigned more than one host retention policy through its host group membership, only the highest precedence policy is assigned. If a host isn't assigned a host retention policy, the default policy is applied.

To manage the precedence of host retention policies:

Falcon Management

1. Go to [Host setup and management > Manage endpoints > Host management](#) , then click the [Host retention policies](#) tab.
2. Click [Edit precedence](#).
3. Click and drag the policy records to the desired order of precedence. The first policy is assigned highest precedence and the last policy is assigned lowest precedence.

Click [Save](#).

View a host's retention info

You can view this retention information for a host:

- The host's currently-applied retention policy: The currently-applied host retention policy is based on the highest-precedence retention policy assigned to the host through host group membership. View the [Host retention policy](#) column on the [Host management](#) page.
- How many days before a hidden host is deleted: The number of days before an inactive hidden host is deleted. This value is the difference of the total days of inactivity allowed minus the number of days the host has already been inactive. The total duration of inactivity allowed depends on the currently-assigned host retention policy. If no policy is assigned, the host is deleted after the system default of 45 days. View the [Permanently deleted](#) in column on the [Hidden hosts](#) page.

1. Go to [Host setup and management > Manage endpoints > Host management](#) .
2. To view a host's currently-applied retention policy, find the applicable host in the table and refer to the [Host retention policy](#) column.
3. To view the number of days before a hidden host is deleted:
 - a. Click the [Hidden hosts](#) tab.
 - b. Find the applicable host in the table and refer to the [Permanently deleted](#) in column.

More info:

- For more info about assigning hosts to host groups, see [Managing host groups](#).
- For more info about assigning host groups to host retention policies, see [Manage settings for a host retention policy](#).
- For more info about setting precedence for host retention policies, see [Manage host retention policy precedence](#).
- For more info about specifying an inactivity period for automatically deleting hosts, see [Manage settings for a host retention policy](#).

Manually hide a host

You can manually hide a host from the console. After a host is hidden, it is moved to the [Hidden hosts](#) page and removed from the other pages of the console. For more info about how detections, events, and prevention settings apply to hidden hosts, see [Understanding host hide and delete actions](#).

Important: Use caution when hiding mobile hosts, they can't be restored. See [Hiding mobile hosts](#).

1. Go to [Host setup and management > Manage endpoints > Host management](#) .
2. Use one of these methods to hide one or more hosts:
 - Select one or more hosts in the [Host management](#) table, then click [Hide hosts](#). You can hide up to 100 hosts at one time.
Tip: To quickly locate your duplicates, hide hosts as part of your re-imaging workflow. Sort the list by the [Hostname](#) field. If multiple hosts share a [Hostname](#) and [Serial number](#) value, the reimaged host is the one with the most recent value in the [Last seen](#) field. Hide the other hosts as duplicates.
 - In the [Hosts](#) tab, locate the applicable host in the table and click [Actions](#) () > [Hide host](#) or open the [Host information](#) panel for that host, then click [Actions](#) > [Hide host](#).

Note: For information about automatically hiding inactive hosts, see [Host retention policies](#).

Restore a host

Hidden hosts can be restored to all pages of the Falcon console.

Important: Mobile hosts are not moved to the [Hidden hosts](#) page when hidden and they can't be restored. Additionally, deleted hosts can't be manually restored, they are automatically restored to the console if they come online. See [Hiding mobile hosts](#).

1. Go to [Host setup and management > Manage endpoints > Host management](#) , then click the [Hidden hosts](#) tab.
2. Restore hosts using one of these methods:
 - To manually restore, select one or more hosts, then click [Restore](#).
 - To automatically restore hidden hosts when they come online, enable the [Auto-restore active hidden hosts](#) setting. When hosts reconnect and are automatically restored in this way, it can take up to an hour for the restored hosts to appear in [Host Management](#).

Detection reporting resumes for the restored hosts. Detections appear in the console from the time before the host was hidden and after it was restored. Events sent during the time the host was hidden don't appear as detections in the console.

A restored host that is inactive can still be automatically hidden or deleted according to the settings of a host retention policy assigned and applied to it. See [Host retention policies](#).

Changing a host's network containment status

From a host's summary panel, you can network contain a Windows, Mac, Linux, iOS, or Android host to isolate it from all network activity.

For more info about containing a host, see [Network Containment](#).

Note: Network containment is not available for ChromeOS hosts.

To change a host's network containment status, in the host's summary panel, click the [Actions](#) menu, and then click [Network contain host](#):

Falcon Management

- Network Contain - click to contain an un-contained host
- Lift Containment - click to un-contain a contained host
- Lift Containment Pending - status is in the process of moving from contained to un-contained
- Containment Pending - status is in the process of moving from un-contained to contained

Note: Only users with specific roles can contain hosts. For more info, see [User Management](#).

Disabling detections on a host

To disable detections on a host, in the host's summary panel, click the Actions menu, and then click Disable detections. This is helpful for users who want to set up hosts to test detections in the Falcon console and who later want to remove those old test detections from the console.

Tip: Instead of disabling all detections on a host, you can set up a detection and prevention policies pattern to prevent detections from appearing for specific file names, paths, and extensions. For more information, see [Detection and Prevention Policies](#).

When active, this feature only suppresses detections for the host. The feature does not disable the sensor or interfere with the sensor's ability to protect the host. Consider the behavior explained below.

- The sensor continues to operate normally except that detections for the host do not appear in the [Endpoint security > Monitor > Endpoint detections](#) feed or in any related email alerts.
- Activity related to the host is still factored into [Endpoint security > Monitor > Endpoint detections](#).
- Configurations such as prevention toggles that are applied to the host from Prevention Policies, prevention hash rules (set in IOC Management), Custom IOA Rule Groups, Exclusion rules, and so on are still processed normally.

When detections are disabled:

- Falcon console impact: The detections for that host are removed from the console immediately. No new detections display in the console going forward unless detections are enabled. If enabled, any detections that existed prior to disabling detections are restored to the console.
- API impact: The `EppDetectionSummaryEvent` stops getting sent to the Streaming API for that host.
- Event Search impact: Even after disabling detections, the data for all existing detections prior to disabling detections still appears in Event Search.

To re-enable detections, click Enable Detections.

When detections are enabled:

- Falcon console impact: New detections start appearing in the console immediately. Any detections that existed prior to disabling detections are restored to the console.
- API impact: The `EppDetectionSummaryEvent` starts getting sent to the Streaming API for that host.
- Event Search impact: Detections will start to appear in Event Search. No detections will be available for the period of time when detections were disabled. The data for any detections for that host that existed prior to disabling detections will remain in Event Search.

Managing host groups

Host groups allow you to assign policy settings, sensor upgrades, file path exclusions, and more to one or more hosts. Hosts can belong to multiple groups so you can tailor policy and other configuration settings to the needs of your environment.

Important: With fine-grained access, users can't manage host groups unless they are assigned All hosts in their user account. This ensures that a user can't grant themselves access to disallowed hosts by updating host groups. For more info, see [Controlling access to data with FGA](#).

There are two types of host groups — dynamic and static. The group type is selected when you create it and can't be changed later.

- Dynamic host groups are empty upon initial creation. To add hosts, define filters based on attributes such as tags, IP/CIDR range, OS version, Active Directory OU, or hostname prefix or suffix. When hosts match the assignment rule for a dynamic group, they are automatically added to the group. When a host no longer matches the assignment rule for the group, it's automatically removed. We recommend dynamic groups in most cases. For more info, see [Planning dynamic host groups](#).
- Static host groups are defined manually. Static groups are useful for hosts in static environments, such as QA or testing, or for when dynamic group filters are insufficient. There is a limit of adding 1,000 hosts to a static group at a time. For more info, see [Assign hosts to a static group](#).

When creating a static host group, you must select whether to add hosts by hostname or host ID (also known as agent ID). This selection can't be changed later. You can add hosts to a static group using any of these methods:

- By selecting hosts using filters in the Falcon console
- By manually entering hosts in the Falcon console
- By uploading a text file containing a list of hosts

Important: For optimal search resolution performance, we recommend that static host groups should contain no more than 10,000 hosts. There are no hard limits on dynamic group membership, but note that search resolution performance for large host groups, such as 100,000-150,000 hosts, might be impacted by the use of multiple or complex targeting criteria instead of the recommended use of minimal targeting criteria.

When creating dynamic or static host groups for containers, use these fields to create the filter specific to pods:

- Pod Name
- Pod ID
- Pod Labels

Note: After you've set up a host group, hosts are dynamically included based on the assignment rules you define. Hosts that match the assignment rules are targeted by the host group. A host group is applied to a targeted host that is online. If an offline host is part of a group when its state no longer matches the assignment rules, or if it's manually removed while offline, the host group is no longer targeting the host, but the host group is still applied to the host until it comes online and is removed from the group. A host must be online for the CrowdStrike cloud to determine whether it still matches the assignment for membership in a host group.

Falcon Management

Planning dynamic host groups

Dynamic groups are flexible so you can tailor your group structure to the specific needs of your environment. You'll use these groups to assign policies to your hosts, so consider different ways you can identify hosts to sort them into the correct groups. Groups can be based on standard attributes, tags, or a combination.

Using standard attributes

Standard attributes are existing traits that can be used as filters to organize hosts. Attributes include IP address/CIDR block, hostname, and Active Directory OU. Possible use cases include:

- Apply more restrictive policies for hosts in your Finance department by creating a dynamic group that filters Hostnames that start with "FIN".
- Disable cloud updating in an office with bandwidth limits by creating a dynamic group assignment rule using the IP/CIDR filter to select only hosts on that office's subnet.

You can add multiple filters to your assignment rule to be more specific about which hosts belong to that group. For example, if you're remediating a suspected incident on hosts in a single department at one office location, you might add multiple criteria to your assignment rule so that the target group is made up of hosts that both:

- belong to a specific departmental OU
- are in the Site Name impacted

Group hosts using tags

Use tags to dynamically assign hosts to host groups based on custom keywords you define. Host group assignment determines which policy is applied to a host. Possible use cases include:

- Apply a less aggressive prevention policy to software engineers by adding a tag to their hosts and creating a group assignment rule with the Tags filter.
- Apply tags based on attributes tailored to your environment to more easily identify and filter hosts in the Host Management and the Detections pages.

Important considerations when using tags:

- Search all fields won't show search results for tags.
- Tag filters are case-sensitive.

Falcon supports these types of tags:

- Falcon grouping tags
- Sensor grouping tags
- Third-party tags

Falcon grouping tags

	Description
Management interfaces	Create, edit, and remove Falcon grouping tags using these interfaces: • Falcon console • CrowdStrike API
Persistence	Falcon grouping tags persist based on the hosts they are assigned to: • If you remove a tag from all hosts, the tag ceases to exist. • If all the hosts with a tag are inactive for 45 days, the tag ceases to exist. In both cases, you can create the tag and assign it to hosts again.
Management considerations	You can manage Falcon grouping tags for hosts individually or in bulk using the Falcon console. These tags are shown with the prefix FalconGroupingTags. You don't need to specify this prefix when creating tags as Falcon adds it automatically. There is a 237 character limit for a tag. You can add up to 50 tags per host and 1000 tags per CID. You can't manage these tags on the sensor using the CLI or using an MDM. You can't use these tags with sensor images or templates.

Sensor grouping tags

	Description
Management interfaces	Manage sensor grouping tags using these interfaces: • MDM for mobile hosts • Sensor CLI for nonmobile hosts
Persistence	Sensor grouping tags persist as long as they are present in any sensor's configuration. If these tags are set in a sensor configuration on an image, the tags persist in sessions created from that image.

Falcon Management

	Description
Management considerations	Sensor grouping tags appear in the Falcon console, however you can't manage them using the console or the CrowdStrike API. These tags are shown with the prefix SensorGroupingTags. You don't need to specify this prefix when creating tags as Falcon adds it automatically. You can use these tags with sensor images and templates. For Falcon sensor for Windows, set tags at sensor installation. Changes after installation require a registry edit and a host reboot; otherwise, the changes take effect when the sensor is next upgraded. For Falcon sensor for Mac and Falcon sensor for Linux, manage tags using the CLI and restart the sensor for changes to take effect. For more info about managing sensor grouping tags, see the relevant deployment guide sections: • Windows: Assigning sensor grouping tags during installation • Mac: Managing sensor grouping tags • Linux: Managing sensor grouping tags • Android: Using tags to identify mobile sensors • iOS: Using tags to identify mobile sensors

Third-party tags

	Description
Management interfaces	View, filter, and sort third-party tags using these interfaces: • Falcon console • CrowdStrike API
Persistence	If a host is removed from the Falcon console due to inactivity, when it reconnects it may take up to 24 hours for any changes to third-party tags to update.
Management considerations	Supported third-party sources: AWS tags for EC2 and EC2 V2 instances. Note: If you're unable to view tags for your EC2 instances, you might need to enable access within AWS. For more info, see the AWS article View tags for your EC2 instances using instance metadata. Third-party tags are available on Windows and Linux hosts running sensor version 7.19 and later. Third-party tags can't be created or modified in any way using the Falcon console or an API. Changes to tags from third-party applications might take up to an hour to appear in the Falcon console. All third-party tags contain a prefix that denotes their source. For example: • Tag as it appears in AWS: cstag-business=sales • Host management displays: AWS/cstag-business/sales

Adding Falcon grouping tags from the host summary panel

Add tags to individual hosts through the host summary panel.

There is a 237 character limit for a tag. You can add up to 50 tags per host and 1000 tags per CID.

Note: For bulk additions, see [Adding Falcon grouping tags in bulk](#).

1. Go to **Host setup and management > Manage endpoints > Host management**.
2. Click the host in the list.
3. In the **Grouping Tags** area of the host summary panel, click the **+** icon (Add Falcon Grouping Tag).
4. Enter or select the tag name and click **Add**. Tags names are case sensitive and you don't need to include the **FalconGroupingTags** prefix.
 - For new tags, enter the name of the tag and press **Enter**.
 - For existing tags, begin typing the name and then select the tag.
5. Continue adding tags as needed.
6. Click **Add tags**.

Removing Falcon grouping tags from the host summary panel

Remove tags from individual hosts through the host summary panel.

Note: Sensor grouping tags — tags created and managed through sensor or MDM — can't be removed from the Falcon console. These tags display in the table but don't have a remove option.

Note: For bulk removes, see [Removing Falcon grouping tags in bulk](#).

Falcon Management

1. Go to [Host setup and management > Manage endpoints > Host management](#).
2. Click the host in the list.
3. In the Grouping Tags area of the host summary panel, locate the tag and click the x icon (Remove Falcon Grouping Tag).
4. Click Apply.

Adding Falcon grouping tags in bulk

You can add tags to one or more hosts without having to open the host summary panel.

There is a 237 character limit for a tag. You can add up to 50 tags per host and 1000 tags per CID.

1. Go to [Host setup and management > Manage endpoints > Host management](#).
2. Select one or more hosts.

You can add tags to up to 1000 hosts at a time.
3. Click Actions and select Add Falcon Grouping Tags.
4. Enter or select the tag name and click Add. Tags names are case sensitive and you don't need to include the FalconGroupingTags prefix.
 - For new tags, enter the name of the tag and press Enter.
 - For existing tags, begin typing the name and then select the tag.
5. Continue adding more tags as needed.
6. Click Add tags.

Removing Falcon grouping tags in bulk

You can remove tags from one or more hosts without having to open the host summary panel.

1. Go to [Host setup and management > Manage endpoints > Host management](#).
2. Select one or more hosts.

You can remove tags from up to 1000 hosts at a time.
3. Click Actions and select Remove Falcon Grouping Tags.
4. Select the tags to remove.
5. Click Remove tags.

Find a host group

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Use the search bar to search for the host group name.
3. Optional. Select Expand search criteria to include the Created by and Modified by fields in your search, in addition to Group name. This allows you to search for host groups that a specific user has created or modified.

View host group details

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Locate the desired host group and use one of these methods to view details:
 - Click the host group row to open the details panel, then click the Details tab to see general host group info and, for dynamic host groups, assignment rule details. Additionally, the header lists the number of hosts that the host group has been applied to and the number of hosts targeted by the host group. You can click each of these numeric values to open the Hosts page with a filter automatically enabled to show the applicable hosts.
 - Click the host group name to open the host group page. The page header shows general host group info and, for dynamic host groups, assignment rule details. The Hosts targeting tab shows the hosts currently added to a static host group, or the hosts currently targeted by the assignment rule for a dynamic host group.

In the details panel or on the host group page, you can also view information about assigned policies and exclusions. See:

- [View and manage assigned policies](#)
- [View assigned exclusions](#)

View and manage assigned policies

View overview information about policies assigned to a host group, and get to more details and actions.

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Locate the desired host group and use one of these methods to view information about assigned policies:
 - Click the host group row to open the details panel, then click the Policies tab.
 - Click the host group name to open the host group page, then click the Policy assignment tab.
3. For each assigned policy, view this info or click the policy name to go to the policy details page.

Falcon Management

- Applied: How many hosts in the host group have the policy applied to them. In the details panel, click this numeric value to open the Hosts page with a filter automatically enabled to show the applicable hosts.
 - Pending: How many hosts in the host group are pending the policy assignment. When they come online, the policy will be applied. In the details panel, click this numeric value to open the Hosts page with a filter automatically enabled to show the applicable hosts.
 - Status: Whether the policy is enabled or disabled. In the details panel, this field is labeled Enabled and shows a check mark if the policy is enabled.
 - Assigned to group: This field appears only in the details panel and indicates if the policy is assigned to this host group.
Tip: A value of N/A appears for default policies because they are not assigned but automatically applied to provisioned hosts when no other policy is applied.
 - Precedence: The precedence assigned to the policy.
 - Platform: This field appears only on the host group page to indicate the platform the policy applies to, such as Windows or Linux. On the details panel,
4. From the host group page only, you can add or remove assigned policies without having to go to the applicable policy pages of the console:
- a. To add a policy, go to the desired policy type and click Add policy.
 - b. Select the desired policy, and then click Assign policy.
 - a. To remove a policy, go to the desired policy type and click Remove policy.
 - b. Select the desired policy, and then click Remove policy.
- For more info about policies, see [Detection and Prevention Policies](#).

View assigned exclusions

View overview information about exclusions assigned to a host group, and get to more details and actions.

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Click the desired host group.
The host group page opens.
3. To view assigned exclusions, click the Exclusions tab. For each assigned exclusion, view basic details or click [Manage exclusions](#) to go to the exclusions details page.
For more info about exclusions, see [Detection and Prevention Policies](#).

Create a host group

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Click [Create new group](#).
3. Enter a name and description. Allowed characters are:
 - a-z
 - A-Z
 - 0-9
 - - (hyphen)
 - _ (underscore)
 - :
 - ;
 - .
 - !
 - Spaces
4. Select a group type: Dynamic, Static by host ID, or Static by hostname.
5. Click [Submit](#).

Assign hosts to a host group

You assign hosts using different processes, depending on the group's type.

- **Dynamic group:** Assign hosts by creating an assignment rule. Hosts that meet the criteria of the assignment rule are automatically targeted by the host group. When targeted hosts are online, the host group is applied to them along with any policies and exclusions assigned to the host group. If an attribute for a host changes, such as removing a grouping tag, and the assignment rule no longer applies to the host, the host is no longer targeted by the host group. If an assignment rule for a dynamic group is updated, the host group no longer targets hosts that don't meet the updated assignment rule criteria. Host group assignment changes are applied to hosts when they next come online.
- **Static group:** Assign hosts directly by host ID or hostname. Hosts can also be manually removed from static host groups.

Note: We recommend using dynamic groups. Using static groups can result in hosts changing security settings if the hostname is changed. Static groups can also result in host duplication in the Falcon console.

Assign hosts to a dynamic group

After you have created a dynamic host group and planned the criteria for including hosts, create or update an assignment rule to assign hosts to the dynamic group.

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Select the dynamic group you want to add hosts to.
The host group page opens.
3. Click [Edit assignment rule](#).
4. In the filter bar, add criteria to define the assignment rule and then click [Update](#) to view hosts that meet the criteria.

Falcon Management

5. Click Save assignment rule to save and apply this assignment rule.

Assign hosts to a static group

As opposed to a dynamic group, you can assign hosts to a static group by selecting existing hosts in the console or by uploading a list of host IDs or hostnames. Whether you upload hosts by ID or name depends on the type of group created, Static by host ID or Static by hostname.

When uploading hosts by hostname, Falcon checks that submitted hostnames match hosts that currently exist in the Falcon console. If you want to add hosts to a group before deploying sensors, you can disable validation.

Note: You can upload a maximum of 1,000 hosts to a static host group at a time.

1. Go to [Host setup and management > Manage endpoints > Host groups](#) .
2. Click the static group you want to add hosts to.

The host group page opens.

3. Select one of these options:

- o Upload a file or enter hosts manually:

- a. Select Upload Hosts.

- b. Add hosts by their IDs or by their hostnames. Enter the hosts one per line, or select a TXT file that contains only host IDs or only hostnames separated by new lines.
Example using IDs:

host-ID1

host-ID2

host-ID3

- c. The hostnames or IDs you specify are automatically validated against existing host records in the console. If one or more hosts are not found, you can copy the list of hosts not found to your clipboard for troubleshooting. If you're adding hosts that are expected to not currently have host records in the Falcon console, select Disable Hostname Validation.

- d. Click Add entries to group.

- o Select hosts in the Falcon console:

- a. Click Add Hosts.

- b. Select the checkbox next to the hosts you want to assign. Apply filters to narrow down the list of displayed hosts.

- c. Click Add hosts to group to assign selected hosts to your group.

- d. Click Confirm.

When you return to your static group, you can see the hosts assigned to the group.

Remove hosts from a static group

Manually remove hosts you don't want to include in a static host group.

1. Go to [Host setup and management > Manage endpoints > Host groups](#) .
2. Click the static group you want to add hosts to.
The host group page opens.
3. On the Host targeting tab, select one or more hosts to remove from the host group. Apply filters to narrow down the list of displayed hosts.
4. Click Remove hosts from group.
5. Click Confirm.

Manage host group assignments from the Hosts page

On the Hosts page, you can manage static host group assignments for a single host or for multiple hosts using a bulk action.

Add or remove a host from a static group

1. Go to [Host setup and management > Manage endpoints > Host management](#) .
2. From the host's Action menu, click Host group assignment and select either:
 - a. Add host to static group
 - b. Remove host from static group
3. In the dialog that opens, select a static group from the list. You can also search for a group by name, ID, creator, or modifier.
4. Confirm your selection.

Add or remove multiple hosts from a static group

1. Go to [Host setup and management > Manage endpoints > Host management](#) .
2. Select one or more hosts in the Host management table.
Note: There is a 100 host limit when you add or remove hosts from a group. To add or remove more than 100 hosts at a time, go to the Host groups tab and select a specific host group.
3. Select either:
 - a. Add hosts to static group
 - b. Remove hosts from static group

Falcon Management

4. In the dialog that opens, select a static group from the list. You can also search for a group by name, ID, creator, or modifier.
5. Confirm your selection.

Deleting a host group

1. Go to [Host setup and management > Manage endpoints > Host groups](#).
2. Select the group you want to delete.

The host group page opens
3. Click [Delete group](#).
4. When prompted, click [Delete Group](#) to permanently delete this group.

Note: Deleting a group does not delete the hosts that were in the group. For info about hiding and deleting hosts, see [Manually hide a host](#).

Protecting your CID with installation tokens

Installation tokens prevent unauthorized hosts from being accidentally or maliciously added to your customer ID (CID). Installation tokens are an optional security measure for your CID. To use installation tokens, you create one or more tokens in the Falcon console or through the API, enable the token requirement, and then provide the tokens to sensors at installation time.

Installation tokens should be kept secret. If a token is accidentally exposed, others could use the exposed token to install hosts to your CID. To prevent this, you can revoke existing installation tokens and generate new ones.

Before you begin

- Sensor requirements:
 - Windows, Mac, and Linux: version 5.31
 - Android: 2020.04.2080100
 - iOS: 2020.04.2
- Role requirements:
 - Falcon Administrator: create and manage installation tokens, enable and disable token requirement
 - Endpoint Manager: create and manage installation tokens

Planning your installation tokens

- Determine if installation tokens are appropriate for your CID.
 - Enabling the requirement for tokens during installation applies across the entire CID.
 - Installation tokens are disabled by default.
- Determine how many tokens you want to use and manage. You can have a maximum of 50 installation tokens, including expired and revoked tokens.
 - If you use a single token, installations are simpler, but all installations are affected if a token expires or is revoked.
 - If you use multiple tokens, creating and updating tokens is more complex, but fewer installations are affected if a token expires or is revoked.
- Decide if tokens should expire.
 - If you set an expiration date on a token, the token can't be used after that date.
 - Use token expiration if your organization requires regular token rotation.
 - If you set expiration dates for your tokens, plan to regularly revisit your token settings and create new tokens as needed.
- Decide a naming convention. You can name and add a descriptive label to tokens, but you can't tie them to a specific platform, host group, or other attribute.

Example token lifecycle

1. A Falcon admin plans how many different tokens their environment needs, such as:
 - A token for Windows hosts, managed using SCCMA
 - A separate token for Linux hosts, managed using Chef
 - A third token for Android and iOS hosts, managed using an MDM platform
2. The admin creates each token in the Falcon console or API.
3. The admin updates the installation script or playbook in each platform's management tool so each installation includes the appropriate token.
4. An SCCM log accidentally exposes the Windows token internally. Just to be safe, the admin revokes the Windows token (but not the other tokens).
5. The admin generates a new Windows token and updates it in their SCCM configuration for future installations.

Falcon Management

How tokens work

- Any endpoints that don't have an active token in their installer aren't assigned an agent ID (AID) from the CrowdStrike cloud, so the installation never completes on that endpoint.
- Installation tokens are checked only when the sensor is installed.
 - Changes to installation tokens have no effect on existing hosts. For example, enabling Require tokens or revoking a token only affects future installations, not your existing hosts.
 - After installation, sensors don't retain the token on disk.
- On Android and iOS, the way installation tokens are handled depends on the enrollment method.
 - Zero-touch enrollment: Tokens are managed the same way as desktop sensors.
 - Manual enrollment: Tokens are managed automatically between the host and the CrowdStrike cloud. Installation tokens for manually enrolled mobile devices aren't visible in the Falcon console or through the API.
- Tokens are not case-sensitive.

Managing your installation tokens

Creating installation tokens

1. Go to [Host setup and management > Deploy > Installation tokens](#).
2. Click **Add token**.
3. In **Add installation token**:
 - a. Enter a descriptive name for this token.

Note: You might want to include information on where your organization uses this token, such as its intended platform or host group.
 - b. Select an expiration date or **Does not expire** to set the token's lifespan.
 - c. Click **Add token**.

It can take a few minutes for a new token to be active for installations. If an installation using a new token fails, wait 3-5 minutes and try again.

Editing installation tokens

1. Go to [Hosts > Installation tokens](#).
2. In the **Actions** column for a token, click **Edit**.
3. Update the token's name or expiration date.
4. Click **Update token**.

Revoking installation tokens

When you revoke a token, it can't be used in sensor installations. Revoked tokens can be restored within 7 days, but after that, they're automatically deleted. Revoking tokens only affects future installations, not existing hosts.

Note: It's possible to revoke all your active tokens, but all future installations will fail if the token requirement is enabled and all tokens are revoked.

To revoke a token:

1. In the Falcon console, go to [Host setup and management > Deploy > Installation tokens](#).
2. In the **Actions** column for the active token, click **Revoke** to immediately revoke the token.

Restoring revoked installation tokens

When you restore a revoked installation token, it can be used again in sensor installations.

To restore a revoked token:

1. In the Falcon console, go to [Host setup and management > Deploy > Installation tokens](#).
2. In the **Actions** column for the revoked token, click **Restore** to immediately restore the token.

Enabling or disabling Require tokens

If **Require tokens** is enabled and an installation doesn't include a token, the installation will fail. **Require tokens** is disabled by default.

The first time you interact with installation tokens, you must create at least one token before you can enable **Require tokens** for all future installations. It can take a few minutes for tokens to become active when you first enable **Require tokens**.

To enable or disable the token requirement, go to [Host setup and management > Deploy > Installation tokens](#), then click the **Require tokens** toggle.

Falcon Management

Installing sensors with installation tokens

When you install a sensor after enabling Require tokens, the installation command must include an additional parameter and an active token. For more info, see our deployment guides for each platform.

- Windows: <your executable file name>.exe /install /quiet /norestart CID=<CCID> ProvToken=ABCD1234
- Mac:
 - As a single command: `sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEF GHIJKLMNOPQRSTUVWXYZ WX ABCD1234`
 - As two separate commands:
`sudo /Applications/Falcon.app/Contents/Resources/falconctl provisioning-token ABCD1234`
`sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEF GHIJKLMNOPQRSTUVWXYZ WX`
- Linux: `sudo /opt/CrowdStrike/falconctl -s --cid=<CID> --provisioning-token=ABCD1234`

On Android and iOS, installation tokens are handled depending on the enrollment method. For manual enrollment, tokens are handled automatically and you don't need to specify a token. For zero-touch enrollment, the token must be configured in AppConfig (for Android devices) or the profile (for iOS devices). For more info, see [Deploying Falcon for Mobile to Android Devices](#) or [Deploying Falcon for Mobile to iOS Devices](#).

Reviewing tokens and actions

In the Falcon console, go to [Host setup and management > Deploy > Installation tokens](#) to see your tokens:

Troubleshooting installation tokens

Installations fail with new tokens

If an installation using a new token fails, wait 3-5 minutes and try again. Though a new token's status is Active, it can take a few minutes for the token to be ready for use.

Log contents when a Windows sensor installation fails

If a sensor installation includes no token or an incorrect token, the installation log includes this error:

```
[0278:16A8][2020-04-14T16:50:01]i000: Falcon was unable to communicate with the CrowdStrike cloud. Please check your installation token and try again.
```

Policies in Falcon

Manage Falcon settings and configurations for host groups by creating and assigning policies.

Overview

Manage Falcon settings and configurations for host groups by creating and assigning policies. When you assign a host group to a policy, the policy applies to all hosts in the host group.

Note: This content covers the majority of Falcon policies. Some policies, such as image assessment and application posture policies, are implemented differently.

How policies work

Policies are used in many CrowdStrike features to bulk manage configurations. Most policy types include a Settings tab where you can adjust, enable, and disable feature settings. When you assign a host group to a policy, the policy applies to all eligible hosts within that host group. Similarly, when you update a policy, the update applies to all eligible hosts assigned to the policy.

Note: If a host belongs to multiple host groups that are assigned to different policies, the policy with the highest precedence applies to the host. For more info, see [Policy precedence and default policies](#).

For example, during an active security incident, you might temporarily move hosts into a host group that's assigned to a prevention policy with strict prevention settings and minimal exclusions. After the threat is cleared, you can remove the hosts from that host group.

Create host groups based on similar characteristics like asset type or criticality to streamline host management. For example, a strict device policy for easily accessible assets might be more appropriate for a host group of laptops than a host group of servers.

Consider these points when assigning host groups to a policy:

- Dynamic host groups might unexpectedly affect policy assignment. If changing conditions cause a host to be added to or removed from a dynamic host group, a different policy might be assigned.
- When a host group is assigned to a policy, hosts in the host group must be online for the policy to apply.
- Policy application might take some time to take effect, depending on the policy type.

For details and procedures regarding an individual policy type, see the specific policy documentation.

Policy precedence and default policies

Each policy type includes a *default policy* that applies to all hosts that don't have an assigned policy. Policies that you create beyond the default policy have an assigned precedence where 1 is highest.

Note: The default policy only applies when a host does not belong to a host group assigned to a policy. You cannot manually assign host groups to a default policy.

If a host is in multiple host groups, the policy with the highest precedence applies. If that policy is deleted or disabled, the policy with the next highest precedence applies.

Falcon Management

Manage policies in the Falcon console

In most cases, policies are listed in a table ordered by precedence. You can create policies and change the order of precedence. Select a policy name to open the corresponding policy details page.

Windows prevention policies

Platform

Windows

5 Windows policies

Edit precedence

Create policy

Precedence	Status	Name	ID	Created	Last Modified	Applied hosts	Pending hosts
1	Enabled	Block all	XXXXXXXXXXXXXXXXXXXX	Aug. 2, 2025 03:39:14	Aug. 2, 2025 03:39:24	44	7
2	Enabled	Monitor only	XXXXXXXXXXXXXXXXXXXX	Jul. 14, 2025 13:57:08	Jul. 14, 2025 13:58:58	79	5
3	Enabled	Prevent - optimized	XXXXXXXXXXXXXXXXXXXX	Jul. 14, 2025 13:59:14	Jul. 14, 2025 14:01:10	29	0
4	Enabled	Detect - optimized	XXXXXXXXXXXXXXXXXXXX	Jul. 7, 2025 01:35:37	Jul. 7, 2025 01:36:57	43	0
	Enabled	Default (Windows)	XXXXXXXXXXXXXXXXXXXX	Nov. 7, 2016 15:34:41	Jun. 4, 2025 23:12:10	16	23

Policy tables typically include these columns:

- **Precedence:** Order of policy precedence where 1 is the highest. If a host is in multiple host groups with different policies, the policy with the highest precedence applies.
Tip: To update the policy precedence order, click Edit precedence.
- **Status:** Whether the policy is enabled. If a policy is disabled, the policy with the next highest precedence applies.
- **Name:** Name of the policy. Click on the link to view the policy details.
- **ID:** CrowdStrike identifier assigned to the policy. IDs can be used to filter API queries.
- **Created:** When the policy was created.
- **Last modified:** When the policy was most recently updated.
- **Applied hosts:** Number of hosts the policy applies to.
- **Pending hosts:** Number of hosts where the policy has not yet been applied. If a pending host is offline, the policy applies when the host comes back on line.

Policy details pages

Select a name in a policy table to open the corresponding policy details page. Here, you can review policy details, update policy configurations, and enable, disable, or duplicate the policy.

Query Machines

Enabled

Standard settings approved for osquery-enabled assets.

Delete policy

Disable policy

Duplicate policy

Platform

Windows

Policy ID

XXXXXXXXXXXXXXXXXXXX

Precedence

1 of 4

Created

Jul. 5, 2025 03:...

Last modified

Jul. 10, 2025 1...

Settings

Assigned host groups

Cancel

Save

Setting name		Description
osquery	☒	Allows osquery-based queries created and initiated by Falcon users with IT automation permissions to execute on hosts. When enabled, CrowdStrike's osquery binary (~20MB) is downloaded on compatible hosts. When disabled, the binary is removed.
Scripts		
Python	☒	Allows Python scripts created and initiated by Falcon users with IT automation permissions to execute on hosts. When enabled, a Python interpreter is downloaded on compatible hosts. When disabled, the interpreter is removed.
PowerShell	☒	Allows PowerShell scripts created and initiated by Falcon users with IT automation permissions to execute on hosts

Note: Duplicate policies inherit the settings of the original policy, but not the host group assignments.

The policy details page might include tabs that are specific for a policy type, but typically the page includes these tabs:

- **Settings:** Features related to the policy that can be enabled, disabled, or configured
- **Assigned host groups:** Host groups that are assigned to the policy

Page 35 of 191

Falcon Management

Assigned host groups

The Assigned host groups tab includes a table of the host groups assigned to the policy. The table typically includes these columns:

- Name: Name of the host group.
- Hosts with this policy applied: Number of hosts in the host group the policy applies to.
- Total hosts in group: Number of hosts in the host group.

The Hosts with this policy applied value might not match the Total hosts in group value for several reasons:

- The host has characteristics that don't match the policy. For example, if the policy is specific to Windows and the asset is Linux based.
- The host is part of another host group assigned to a policy with a higher precedence.
- The policy is pending for hosts in the host group. For example, a host was offline when the host group was assigned to the policy. The policy is applied when the host comes back online.

Host group policy assignment details

From the Assigned host groups tab, click the name of a host group to view details. The Host data section shows aggregates of how the policy is applied:

- Hosts with policy applied: Number of hosts the policy applies to.
- Hosts with policy pending: Number of hosts where the policy has not yet been applied. If a pending host is offline, the policy applies when the host comes back online.
- Hosts using other policy: Number of hosts in the host group assigned to a different policy. This might occur if an assigned policy has a higher precedence or if the asset platform doesn't match the policy platform.

Server Group West

Host data

Hosts with policy applied	3
Hosts with policy pending	2
Hosts using other policy	3
Total hosts	8

Hosts using other vulnerability management policies - 3 ⓘ

Precedence	Policy name	Platform	Hosts
3	Linux Server Policy	Linux	25

CloseView host group detail page

Falcon Browser Extension

Monitor files and data uploaded or downloaded in a browser. Configure Falcon browser extension settings.

Overview

Web-based data exfiltration is one of the most common channels for data loss. The Falcon browser extension monitors files and data uploaded or downloaded in a browser. As an admin, you can stop end users from uploading files and clipboard data to websites and cloud applications.

There are two versions of Falcon browser extension.

Falcon Management

Falcon browser extension v2:

- Protects against data exfiltration.
- Device Trust support for Identity Protection Cloud access triggers is available.
- Installation settings are customizable.
- Data Protection policies can be configured to control browser extension behavior.

Falcon browser extension v1:

- Protects against data exfiltration.
- Installation is automatic.

Note: Falcon browser extension v1 is being replaced by v2. Browser extension v1 will be deprecated when Falcon sensor 7.24 is no longer supported.

Falcon browser extension v2

The Falcon browser extension v2 enables web-focused features in Falcon Data Protection, as well as device trust support for the Identity Protection Cloud access trigger.

Requirements: Falcon browser extension v2

Requires all of these subscriptions:

- Falcon Insight XDR

Requires one of the following subscriptions:

- Falcon Data Protection
- Falcon Identity Threat Protection

Server support:

- Windows Server 2016 or later
- macOS Ventura or later

Sensor support:

The Falcon sensor must be installed on your endpoints. For more info, see [Falcon Sensor for Windows Deployment](#).

- Windows: Falcon sensor 7.25 and later
- macOS: Falcon sensor 7.26 and later

Note: When you update your Falcon sensor from 7.24 to 7.25 or later, your browser extension is also automatically upgraded to v2.

System requirements:

- Workstations with Windows 10 and later. For more info, see [supported 64-bit versions of Windows 10](#). For US-GOV-1 and US-GOV-2 customers, see [supported 64-bit versions of Windows 10](#). Arm64 is not supported.
- Workstations with macOS Ventura 13 and later

Supported browsers:

All browsers must be managed by your organization.

- Google Chrome: latest three major release versions
- Microsoft Edge: latest three major release versions

Default roles:

- Falcon Admin (read and write)
- Data Protection Admin (read and write) (only needed to configure Data Protection settings)
- Data Protection Analyst (read only)
- Falcon Host Administrator (read and write)
- Falcon Host Read Only (read only)
- Falcon Security Lead (read only)

CrowdStrike clouds: Available in all clouds

Before you begin

[Host groups](#) are required to assign policy settings, upgrades, and file path exclusions, to one or more hosts. Host groups are usually created during sensor installation. For more info, see [Host and Host Group Management](#).

A browser extension policy is required if you are enforcing Data Protection settings.

Setup: Falcon browser extension v2

Custom installation is available for macOS and Windows. Automatic installation is available for Windows, but is turned off by default. All browsers must be managed by your organization.

Falcon Management

- Custom installation: Mac
- Custom installation: Windows
- Automatic installation: Windows

Custom installation: Mac

Admins can force-install the browser extension v2 using the mobile device management (MDM) of their choice. For example, [Jamf Pro](#).

You need the extension URL and extension ID.

- Extension URL: <https://update-crx.falcon.crowdstrike.com/v2/update.xml>
- Extension ID: k1icnoc1cmhafeeepkpdedpojllaaf1f

Create a browser extension policy

For macOS, you do not have to create a browser extension policy and assign it to host groups. The default policy, which is automatically assigned to all relevant hosts, is sufficient.

If your organization would like to create a browser extension policy, do the following.

1. In the Falcon console, go to Host setup and management > Browser extension policies.
2. Click Create policy.
 - a. Enter a name and description and click Create policy.
3. Click the Assigned host groups tab.
4. Click Assign host groups to policy.
 - a. Select the host groups you want to use in this policy.

You can search for a host group by typing its name in the search bar. You can also click Add New Group to create a host group.
 - b. Click Assign group.

Install the Falcon browser extension and the Falcon sensor

1. Use the mobile device management (MDM) of your choice to install the extension to your users' machines.
2. Install the Falcon sensor to your user's machines. For more info, see [Falcon Sensor for Windows Deployment](#).

Custom installation: Windows

Admins can force-install the Falcon browser extension v2 using the mobile device management (MDM) of their choice. For example, [Microsoft Intune](#) or [Workspace ONE](#).

Your instance must be joined to a Microsoft Active Directory domain, a Microsoft Entra ID, be MDM-managed, or enrolled in Chrome Browser Cloud Management.

You need the extension URL and extension ID.

- Extension URL: <https://update-crx.falcon.crowdstrike.com/v2/update.xml>
- Extension ID: k1icnoc1cmhafeeepkpdedpojllaaf1f;

Create a browser extension policy

1. In the Falcon console, go to Host setup and management > Browser extension policies.
2. Click Create policy.
 - Enter a name and description and click Create policy.
3. Click the Assigned host groups tab.
4. Click Assign host groups to policy.
 - a. Select the host groups you want to use in this policy.

You can search for a host group by typing its name in the search bar. You can also click Add New Group to create a host group.
 - b. Click Assign group.

Install the Falcon browser extension and the Falcon sensor

1. Use the mobile device manager of your choice to install the extension to your users' machines.
2. Install the Falcon sensor to your users' machines. For more info, see [Falcon Sensor for Windows Deployment](#).

Automatic installation: Windows

Your instance must be joined to a Microsoft Active Directory domain, a Microsoft Entra ID domain, be MDM-managed, or enrolled in Chrome Browser Cloud Management.

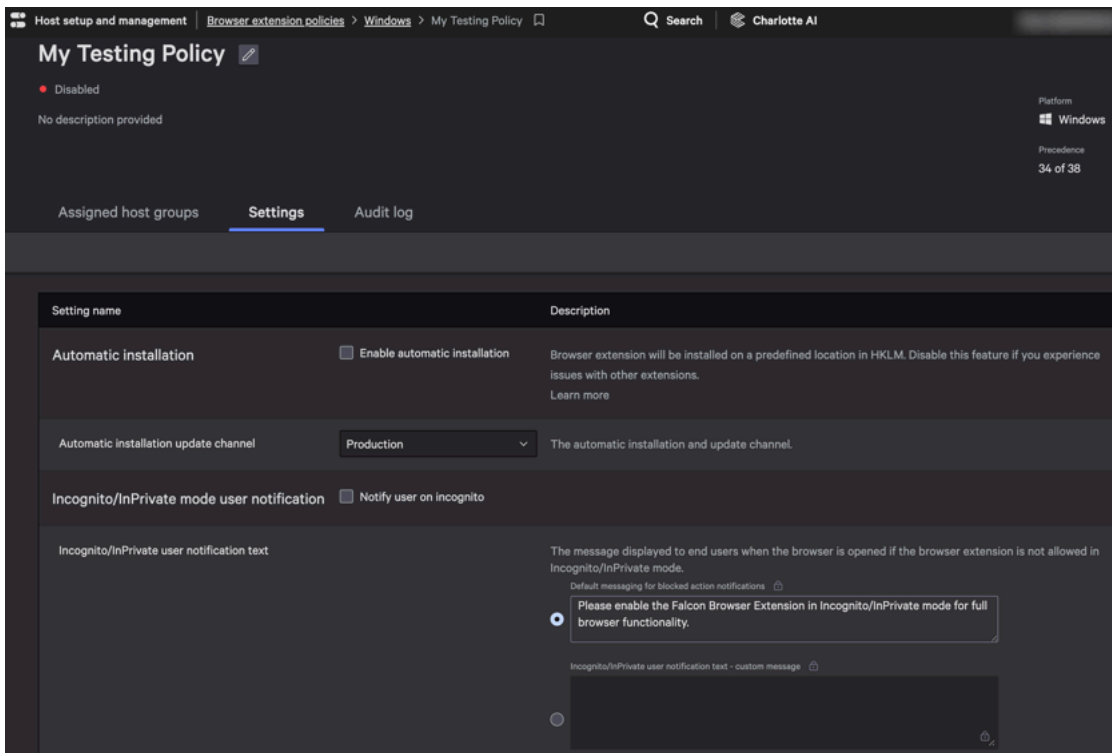
You can turn on automatic installation by creating a browser extension policy and enabling automatic installation.

Tip: For info about how policies work, including host group assignment and policy precedence, see [Policies in Falcon](#).

Falcon Management

1. In the Falcon console, go to Host setup and management > Browser extension policies.
2. Click Create policy.
 - a. Enter a name and description and click Create policy.
3. Click the Assigned host groups tab.
4. Click Assign host groups to policy.
 - a. Select the host groups you want to use in this policy.

You can search for a host group by typing its name in the search bar. You can also click Add New Group to create a host group.
 - b. Click Assign group.
5. Open the browser extension policy and click the Settings tab.
6. Go to Automatic installation and click the checkbox. Select an Automatic installation update channel.



The Falcon browser extension is automatically installed to Google Chrome and Microsoft Edge on your users' machines when the Falcon sensor is installed.

You may need to allowlist the extension ID: `klicnoc1cmhafeeepkpdedpojllaaf1f`;

Configure Falcon browser extension v2 policy settings

Open the Falcon browser extension policy and click the Settings tab. Admins can configure the following settings.

Automatic installation

Automatic installation is only available for Windows.

Click the checkbox to turn on automatic installation. The browser extension is installed on user endpoints.

Automatic installation update channel

Use the dropdown menu to choose the installation and update channel.

Override extension location

This checkbox is disabled by default. If it is enabled, CrowdStrike Customer Support has enabled a custom installation URL for the extension, for debugging or testing purposes.

Custom extension location

This field is empty by default. If it is not empty, CrowdStrike Customer Support has enabled a custom installation URL for the extension, for debugging or testing purposes.

Incognito/InPrivate mode user notification

When this checkbox is enabled, users will receive a notification if they open a browser and the browser extension is not enabled in Incognito or InPrivate mode. This notification reminds the user that they need to enable the extension for full browser capabilities. The notification is not displayed when the extension is enabled in Incognito or InPrivate mode. The Incognito/InPrivate mode enablement is persistent.

Incognito/InPrivate user notification text

You can use the default notification text or create your own.

Falcon Management

Manage Falcon browser extension settings related to Data Protection

To configure these settings, see [Configure Data Protection Policy Settings](#).

Falcon browser extension v1

The Falcon browser extension v1 is solely a Data Protection feature. It protects against data exfiltration. You cannot configure any settings if you are using browser extension v1.

Note: Browser extension v1 is being replaced by v2. Browser extension v1 will be deprecated when Falcon sensor 7.24 is no longer supported.

Requirements: Falcon browser extension v1

Requires all of these subscriptions:

- Falcon Insight XDR
- Falcon Data Protection

Sensor support:

- Falcon sensor 7.25 and later. The Falcon sensor must be installed on your endpoints. For more info, see [Falcon Sensor for Windows Deployment](#).

Note: When you update your Falcon sensor from 7.24 to 7.25 or later, your browser extension is also automatically upgraded to v2.

System requirements:

- Workstations with Windows 10 and later. For more info, see [supported 64-bit versions of Windows 10](#). For US-GOV-1 and US-GOV-2 customers, see [supported 64-bit versions of Windows 10](#). Arm64 is not supported.

Supported browsers:

All browsers must be managed by your organization.

- Google Chrome: latest three major release versions
- Microsoft Edge: latest three major release versions

Detailed visibility is limited in unsupported browsers.

Default roles:

- Falcon Admin (read and write)
- Data Protection Admin (read and write)

CrowdStrike clouds: Available in all clouds

Setup: Falcon browser extension v1

Falcon browser extension v1 is installed automatically when a Falcon Admin assigns a host group to a non-default Data Protection policy. The host must be Active Directory (AD) joined or have mobile device management (MDM). In some cases, organizations may need to add the extension ID to an allowlist. The extension ID is: obojlibenopmhbbffmmcimgingecokj

Limitations

- Falcon browser extension v1 is only available for Windows.
- You cannot configure installation settings or Data Protection settings.

Upgrade from browser extension v1

When you update your Falcon sensor from 7.24 to 7.25 or later, your browser extension is also automatically upgraded to v2.

Falcon Notifications

Learn about the notification options to let you know about detections, policy changes, cloud security findings, and more, even when you're not logged in to the Falcon console.

Overview

Falcon has a number of notification options to let you and other members of your organization know about things like incidents, detections, policy changes, cloud security findings and more. This is helpful for staying up to date even when you're not logged into the Falcon console.

Falcon notifications comparison

Notification type	Covers	Distribution method	What you control
Fusion SOAR	Incidents	Webhook	You control everything: -Precise trigger and conditions -Notification content -Email recipients/notification channels
	Detections	Email	
	Policies	Slack	
	Cloud security findings	PagerDuty	
		Microsoft Teams	

Falcon Management

Notification type	Covers	Distribution method	What you control
Standard incident and detection notification emails	Incidents Detections	Email	The addresses on the email distribution list
Notification options for case management	Cases	Webhook Email Slack PagerDuty	Email recipients/notification channels
Scheduled Searches	Endpoint event data and sensor events Event data collected from integrated third-party sources	Webhook Email Slack PagerDuty Microsoft Teams	You control everything: -Precise trigger and conditions -Notification content -Email recipients/notification channels
OverWatch incident notification emails	OverWatch incidents	Email	View and request updates to your OverWatch notification contacts list
Intelligence news and report subscriptions	Intelligence news and reports based on your subscriptions	Email	Manage your personal subscriptions
Falcon Malquery Monitoring Rule results	Results matching your YARA rules	Email	Opt to get instant, daily, or weekly email notifications for any YARA rule

For product communication including release notes and tech alerts, visit the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, visit the [CrowdStrike Government Customer Center](#).

Standard Incident and detection notification emails

CrowdStrike sends email notifications about incidents and detections to your specified recipients.

- CrowdScore incidents: CrowdStrike sends an email notification for each new incident when it reaches a score of 1.0 or higher.
- Detections: CrowdStrike sends one email notification for each detection with a severity of low or higher. To quiet detections for expected and trusted activity, create an exclusion.
- See also: [OverWatch incident email notifications](#)

To turn off notifications for incidents, open a [Support case](#). For US-GOV-1 and US-GOV-2 customers, open [Support case](#).

Requirements

- Subscription: Available with Falcon Insight XDR and Prevent
- Sensor support: All Falcon sensors for Windows, macOS, and Linux
- Roles: Falcon Administrator can manage recipients for incident and detection notification emails.
- Recipients: Send incident and detection notification emails to anyone in your organization
- Clouds: Available in all clouds.

Planning standard incident and detection notification email recipients

Standard incident and detection notification emails can contain sensitive identifying information about your environment, such as host names. For security reasons, we recommend using email addresses from only the domains that you control. Using email addresses from domains outside of your control could introduce security risks.

Consider who should receive notifications to support your broader incident-response process. Email notifications can serve as important alerts about suspicious activity and potential attacks.

You can specify an unlimited number of email recipients. To simplify maintenance, we recommend using distribution lists instead of individual email addresses.

Your configured email notification recipients will receive notifications about both incidents and detections.

After you set up the list of recipients, confirm that the correct email addresses are receiving the necessary notifications about incidents and detections.

Add the *crowdstrike.com* domain to your email allowlist to ensure that notification emails aren't blocked by spam filters.

Falcon Management

Managing standard incident and detection notification email recipients

To ensure that your standard incident and detections notification emails are only sent to trusted recipients, check the entered email addresses carefully. We also recommend that you review your configured email recipients periodically.

If you remove a recipient's address from the list, that recipient might continue receiving email notifications for a short period of time until the changes fully take effect.

These email recipient settings don't apply to Falcon OverWatch alerts. To manage your OverWatch alert recipients, contact Support.

Manage incident and detection email recipients:

- Go to Support and resources > Resource and tools > General settings, click Notifications, under Detection and incident emails, enter the email addresses that CrowdStrike will send notifications to.

Detection and incident emails

Manage which addresses get notified about detections and incidents. Consider using a distribution list if addresses change often. Emails are typically sent once per day for each detection at Medium severity or incident at 1.0 and above. [About detection and incident emails](#)

Send email notifications to

Save

OverWatch incident email notifications

Requirements:

Subscription: Falcon OverWatch

Understanding notifications from OverWatch

CrowdStrike sends an email notification to your designated OverWatch email recipients whenever OverWatch analysts create or update an incident. The email contains a direct link to the relevant incident in the Falcon console, where you can begin your investigation and remediation process.

If OverWatch analysts update an incident that you've closed, you'll still receive an email notification about the update. If you want to restart your investigation and remediation process, you can reopen the incident in the Falcon console.

View your OverWatch contacts through the OverWatch Activity dashboard at Dashboards and reports > Dashboards > All dashboards.

Learn more about OverWatch in the Falcon OverWatch Guide.

Intelligence news and reports

Overview

Falcon Intelligence delivers emails based on user subscriptions. Read more about managing these subscriptions in the Falcon Intelligence Overview.

Requirements

Subscription: Falcon Intelligence

Roles: See Roles for Falcon Intel and Falcon Sandbox

Falcon MalQuery Monitoring Rule results

Overview

MalQuery updates its malware sample repository each day. In Threat intelligence > Monitor > Malquery monitoring rules see your saved YARA hunts. You can also choose to run them periodically and send email notifications when new results are found. Read more about managing your monitoring rules in the Falcon Malquery Feature Guide.

Requirements

Subscription: Falcon MalQuery

Roles: MalQuery Admin or MalQuery User role

Detection Attribute Management

Overview

Detection attributes provide detailed information and context about a detection. Customize which detection attributes appear in the list view of identity, endpoint, mobile, data protection, and unified detections. Customizing detection attributes narrows the set of attributes you see when reviewing detections, helping you triage more quickly and easily. Detections attribute templates ensure your preferred attributes are always visible for specific types of detections.

Requirements

- Subscription:
 - Falcon Insight XDR and at least one of these additional subscriptions:
 - For mobile detections: Falcon for Mobile
 - For identity-based detections: Falcon Identity Threat Detection or Falcon Identity Threat Protection
- Default roles:
 - Falcon Administrator
 - All roles that can view and manage relevant detections
- CrowdStrike clouds: Available in US-1, US-2, and EU-1
- Additional requirements for third-party integrations:
 - Your CID must have the required connector for each integrated third-party data source.
 - For more info about third-party integration requirements, see the CrowdStrike documentation for your applicable integrations: [Third-Party Data Sources](#).

Setup

No setup required. Configuring detection attributes is not required.

Managing detection attributes

When you configure which attributes appear for a detection, your changes persist across pages where you view the detection, for example, on Endpoint detections and Next-Gen SIEM unified detections. When you configure attributes for detections, a detection attribute template is automatically created for detections with the same category, source, and properties. Detections attribute templates ensure your preferred attributes are always visible for specific types of detections.

Configure detection attributes

1. Go to detections:
 - Unified detections: [Next-Gen SIEM > Monitor and investigate > Detections](#)
 - Endpoint detections: [Endpoint security > Monitor > Endpoint detections](#)
 - Mobile detections: [Endpoint security > Monitor > Mobile detections](#)
 - Identity-based detections: [Identity protection > Monitor > Identity-based detections](#)
 - Data protection detections: [Data protection > Monitor > Data protection detections](#)
2. Click the  menu of the detection you want to configure, and then select [Configure attributes](#).
3. From the [Configure detection attributes](#) dialog:
 - Optional. Click [See affected detections](#) for a list of detections impacted by changes to the detection attributes.
 - Optional. Select [Configure attributes for all detections from source product](#).
 - Optional. Click the  icon to remove selected attributes.
 - Optional. Add an attribute by typing its name in [Search attributes](#) or clicking the  icon for an attribute.
4. Click [Save](#). The detections list updates with the attributes you added. A detections attribute template is automatically created.

View and manage detections attribute templates

View detections attribute templates

1. Go to detections:
 - Unified detections: [Next-Gen SIEM > Monitor and investigate > Detections](#)
 - Endpoint detections: [Endpoint security > Monitor > Endpoint detections](#)
 - Mobile detections: [Endpoint security > Monitor > Mobile detections](#)
 - Identity-based detections: [Identity protection > Monitor > Identity-based detections](#)
 - Data protection detections: [Data protection > Monitor > Data protection detections](#)
2. Click [Manage detection attribute templates](#) .
3. Optional. Use the filter options to search for a specific detections attribute template.

Edit detections attribute templates

1. Go to detections:

Falcon Management

- Unified detections: [Next-Gen SIEM > Monitor and investigate > Detections](#)
 - Endpoint detections: [Endpoint security > Monitor > Endpoint detections](#)
 - Mobile detections: [Endpoint security > Monitor > Mobile detections](#)
 - Identity-based detections: [Identity protection > Monitor > Identity-based detections](#)
 - Data protection detections: [Data protection > Monitor > Data protection detections](#)
2. Click Manage detection attribute templates .
 3. Optional. Use the filter bar at the top to search for a specific detections attribute template.
 4. From the open menu  of the template, click Edit. The Configure detection attributes dialog opens.
 5. Review the detection properties and number of detections affected by changes to the detection attributes.
 6. Optional. Click See affected detections to view a list of detections impacted by changes to the detection attributes.
 7. Optional. Click Configure attributes for all detections from source product.
 8. Optional. Remove currently selected attributes by clicking the X for the attribute.
 9. Optional. In Search attributes, start typing the name of an attribute you want to add.
 10. Click the plus icon  for the attributes you want to add.
 11. Click Save. The detections list updates with the attributes you added. A detections attribute template is automatically created.

Delete detections attribute templates

1. Go to detections:
 - Unified detections: [Next-Gen SIEM > Monitor and investigate > Detections](#)
 - Endpoint detections: [Endpoint security > Monitor > Endpoint detections](#)
 - Mobile detections: [Endpoint security > Monitor > Mobile detections](#)
 - Identity-based detections: [Identity protection > Monitor > Identity-based detections](#)
 - Data protection detections: [Data protection > Monitor > Data protection detections](#)
2. Click Manage detection attribute templates .
3. Optional. Use the filter bar at the top to search for a specific detections attribute template.
4. From the open menu  of the template, click Delete.

See detections affected by a detections attribute template

1. Go to detections:
 - Unified detections: [Next-Gen SIEM > Monitor and investigate > Detections](#)
 - Endpoint detections: [Endpoint security > Monitor > Endpoint detections](#)
 - Mobile detections: [Endpoint security > Monitor > Mobile detections](#)
 - Identity-based detections: [Identity protection > Monitor > Identity-based detections](#)
 - Data protection detections: [Data protection > Monitor > Data protection detections](#)
2. Click Manage detection attribute templates .
3. Optional. Use the filter bar at the top to search for a specific detections attribute template.
4. From the open menu  of the template, click See affected detections. The list of affected detections opens.

Users and Roles

User Management

Manage your Falcon users, their roles, and their access settings.

Overview

Manage your Falcon users, their roles, and their access settings.

Requirements

Roles

- To create users and assign roles to them, you must have an administrative role, such as Falcon Administrator.
- The Falcon Security Lead can reset user passwords and MFA, but cannot manage users or user roles.

Falcon Flight Control

- Administrators whose home CID is the parent CID can view and manage users in the parent CID and in immediate child CIDs they have access to.
- When working in the parent CID, you can only view and assign users to the child CIDs you have access to.

Falcon Management

Understanding CIDs

In Falcon, a CID (or customer ID) represents a customer account. The CID contains everything relevant to a customer, such as its product subscriptions, data, and users. Depending on the structure and goals of your organization, you can deploy Falcon in 2 configuration models:

- **Standalone CID:** A standalone CID deployment contains all resources, data collection and processing, and users in one account. This model provides easy management with all work and updates happening in one place.
- **Falcon Flight Control (FCTL):** In a FCTL deployment, multiple CIDs are arranged in a hierarchy. This model allows global visibility and operations across all child CIDs from a central parent CID as well as local self-management for each child CID individually.

Home CID

Every user account has a home CID. The home CID is where a user account is created, stored, and managed. The home CID's configured authentication method, or Falcon credentials (SSO if set up by Support), is used for authentication and logging in to the Falcon console. For more info, see [Single Sign-On \(SSO\) for Falcon](#).

The home CID is defined during user account creation. Your deployment model determines how the home CID is assigned. After a user account is created, the home CID cannot be changed.

- **Standalone CIDs:** When a user is created in a standalone CID, that CID is the user's home CID. There is no option to choose a different home CID in standalone accounts.
- **FCTL parent CID:** The home CID for Falcon Flight Control parent users is the parent CID.
- **FCTL child CIDs:**
 - When a child CID user is created from the parent CID, you can designate which child CID will be the home CID.
 - When a user is created locally in a child CID, that child CID is the user's home CID. There is no option to choose a different home CID.

Accessing multiple CIDs

User accounts use one set of credentials to access multiple CIDs. Once you've signed in to your home CID, you have automatic access to any other CIDs associated with your user account.

To change CIDs, on the navigation bar, click the current CID name and select the CID you want to access from the CID list. You can only work in one CID at a time. If you have multiple browser tabs open, they all update when you switch CIDs.

Understanding user accounts

A user account contains attributes that identify a user and determine which resources they can access. It defines the user's name, the unique email address that's used to log in to Falcon, and the roles, groups, and CIDs the user is assigned to.

A unique user account is required for every person in your organization who needs access to the Falcon console. In a Flight Control environment, if a user requires access to more than one CID, you can associate the same user account with multiple CIDs in the Flight Control deployment.

Unique email address

A user account is identified by its email address. When adding a new user account, the email address must be unique, it cannot be used by another user or added in another CID.

Approved domains

Falcon uses your CID's allowed domain list to add users. All user accounts that have access to your CID must be created with an email address from the list of approved domains. For example, if a user's email address is `user@example1.com`, the `@example1.com` domain must be registered in the CID's domain allowlist.

Note: The domain allowlist is configured during a CID's initial provisioning. To make changes to this list, contact Support.

Understanding access control

The Falcon console uses role-based access control (RBAC) to define user access to everything in the Falcon console. A user is assigned one or more roles based on the console functionality relevant to their daily business activities, such as Cloud Security Manager. Each role includes permissions that grant access to perform actions on console resources, such as Read device details.

Fine-grained access (FGA) is a layer on top of RBAC used to further restrict a specific user's access to a subset of resources allowed by their role.

For example, you can use FGA with RBAC to assign user access to these Falcon resources:

Resource	RBAC	FGA
Hosts and host data	A user is assigned one or more roles granting access to hosts.	The user's access to hosts is narrowed only to hosts that belong to one or more host groups the user is explicitly assigned using FGA.
Cloud assets and image attributes	A user is assigned one or more roles granting access to cloud assets and image attributes.	The user's access to cloud security data is narrowed only to cloud assets and images that belong to one or more cloud groups the user is explicitly assigned using FGA.
Next-Gen SIEM detections	A user is assigned one or more roles granting access to detections.	The user's access to detections is narrowed to only those that match the data connection and vendor defined in the assigned access scope.
Advanced event search data	A user is assigned one or more roles granting access to advanced event search.	The user's access to advanced event search data is narrowed to only that which matches the data connection and vendor defined in the assigned access scope.

For more info, see [Controlling access in the console with user roles](#) and [Controlling access to data with FGA](#).

Falcon Management

Controlling access in the console with user roles

User roles determine what a user can see and do in the Falcon console. Every Falcon user is required to have at least one role, which is assigned when a user account is created.

User roles are granted at the CID level, and you can have different roles in each CID you're associated with. In each CID, you have access to all of the features that your roles allow.

Each role includes permissions to perform actions on console resources, which represent anything in the console that can be viewed or managed, such as hosts, policies, firewall rules, user accounts, settings, workflows, and much more. Roles are designed to include a collection of permissions that are required for a type of user, such as a Custom IOAs Manager, to perform their daily business activities in the console without giving the user access to permissions not required to perform those activities.

You can view and manage roles. For more info about roles and permissions, see [Managing access for user accounts](#).

Use temporary roles to grant and revoke access

As a Falcon Administrator, you can limit access to sensitive information and features by granting temporary roles to your users. With these temporary roles, you can escalate privileges for only a specific duration so that your users can perform critical actions or access more sensitive data, such as during incident remediation.

You can grant temporary role access for 1 hour up to 7 days. When the temporary role reaches its duration limit, it expires and is automatically revoked. Every role in your CID is available as a temporary role. For more info, see [Role Management](#).

Note: Foundry roles are not available as temporary roles.

Role assignment types in Flight Control

In Flight Control user accounts, the Assignment type indicates how a role was assigned to the user. This field is displayed on the User management page and the User details page.

There are two types of role assignment:

- Directly assigned: Roles that are assigned directly to a CID.
- Inherited (FCTL): Roles that are assigned through user group or default CID group membership.

Controlling access to data with FGA

Fine-grained access (FGA) is a layer on top of RBAC used to further restrict a specific user's access to a subset of resources allowed by their role.

You can use FGA to narrow access to these Falcon resources:

- Hosts and host data: Explicitly define access to hosts and host data by host group assignment. A user doesn't have access to a host unless that host belongs to at least one host group the user is assigned.

To grant a user access to all hosts, regardless of which host groups they belong to, assign a value of All hosts. Users can only manage host groups if they are assigned All hosts. This ensures that a user can't grant themselves access to disallowed assets by updating host groups.

For more info about host groups, see [Managing host groups](#).

Important: Currently, you can only use FGA to refine host access in host management, host groups, endpoint detections, and real time response (RTR). Users can still see information about all hosts in CrowdScores, event search, and other pages, regardless of the host groups they are assigned. However, in these areas of the console where a user can see all hosts, they are unable to perform host management actions, such as running RTR scripts, if they don't have access to those hosts through FGA.

- Cloud assets and image attributes: Explicitly define access to cloud security asset data by cloud group assignment. A user doesn't have access to cloud security asset data unless the asset is selected by a cloud group the user is assigned.

To grant a user access to all cloud groups, assign a value of All cloud groups.

- Next-Gen SIEM detections: Use access scopes to explicitly define access to detections by data connection and vendor.

Note: In order to access endpoint detections, a user must also have a host group assignment that gives them access to the host.

- Advanced event search data: Explicitly define access to data in advanced event search, whether generated by CrowdStrike or by third-party data connections.

For more info about roles, see [Managing access for user accounts](#).

FGA for hosts and Flight Control

FGA integrates seamlessly with multi-CID environments and Flight Control.

- Managing user host group access: Falcon administrators can manage user host group assignments per CID from the parent CID User management page.
- Viewing and managing hosts:
 - In a parent CID: A user can only view and manage hosts, including performing RTR actions, in a parent CID if the hosts belong to at least one host group the user is assigned in any CID.
 - In a child CID: A user can only view and manage hosts, including performing RTR actions, in a child CID if the hosts belong to at least one host group the user is assigned in that CID.

For more info about Flight Control, see [Falcon Flight Control and Multi-CID Support](#).

Managing users

Create new users and manage existing user accounts, including user access control, password, and MFA settings.

Add users

Add new user accounts to the Falcon console, including assigning access control, assigning host groups and cloud groups, and managing Flight Control and multi-CID access.

Add a user in a standalone CID or child CID

1. Go to [Host setup and management](#) > [Falcon users](#) > [User management](#) , then click [Create User](#).

Falcon Management

2. Enter the user's email address, first name, and last name. If you're planning to enable single sign-on (SSO), the user's email address must exactly match the information in your IdP.
3. Select one or more roles. At least one non-temporary role is required for each user account. For more info about roles and permissions, see [Role Management](#).

Note: Only default roles associated with your subscriptions appear, as well as any custom roles created for your CID.
4. Select one or more host groups to give the user access to. Only hosts that belong to a host group you assign appear in host management or real-time response (RTR). To give access to all hosts, regardless of host group, select All hosts. New user accounts don't have access to any hosts until they are assigned at least one host group. For more info about FGA, see [Controlling access to data with FGA](#).
Important: Users can't manage host groups unless they are assigned All hosts. This ensures that a user can't grant themselves access to disallowed hosts by updating host groups. For more info about host groups, see [Managing host groups](#).
5. Select one or more cloud groups to give the user access to. Users can see only the cloud assets that match the attributes in the cloud groups assigned to them. To give access to all cloud assets, regardless of cloud group, select All cloud groups. Users can't manage cloud groups unless they are assigned All cloud groups. For more info about cloud groups, see [Controlling access to cloud assets and images \(Legacy\)](#).
6. Select one or more access scopes to assign to the user. For more info about access scopes, see [Controlling access to data with FGA](#).
7. Click Save.

Add a user from the Flight Control parent CID

From the parent CID, you can add and configure user accounts for both parent and child CID users and assign them roles. During the user creation process, you can specify the home CID of child users, grant child CID users access to multiple CIDs, add parent CID users to existing user groups, and assign host groups and cloud groups.

1. Go to [Host setup and management > Falcon users > User management](#) , then click Create User.
2. Select Parent CID or Child CID to set where the user account is created.
3. If you're adding a user to a child CID, select from the list of available CIDs to set the user's Home CID. (The parent CID is set as the home CID by default for parent users.)
4. Enter the user's email address, first name, and last name, and then click Next.
5. Select one or more non-temporary roles. At least one non-temporary role is required for each user per CID. For more info about roles and permissions, see [Role Management](#).
6. Select one or more host groups to give the user access to. Only hosts that belong to a host group you assign appear in host management or real-time response (RTR). To give access to all hosts, regardless of host group, select All hosts. New user accounts don't have access to any hosts until they are assigned at least one host group.

For more info about FGA, see [Controlling access to data with FGA](#). For more info about FGA host access in parent and child CIDs, see [FGA for hosts and Flight Control](#).

Important: Users can't manage host groups unless they are assigned All hosts. This ensures that a user can't grant themselves access to disallowed hosts by updating host groups. For more info about host groups, see [Managing host groups](#).

7. Select one or more cloud groups to give the user access to. To give access to all cloud security data , regardless of cloud group, select All cloud groups. New user accounts don't have access to any cloud security data until they are assigned at least one cloud group.

For more info about FGA, see [Controlling access to data with FGA](#).

Important: Users can't manage cloud groups unless they are assigned All cloud groups. This ensures that a user can't grant themselves access to disallowed cloud assets and images by updating cloud groups.

8. Optional. For a user being added to a parent CID, add the user to one or more existing user groups.
9. Optional. For a user being added to a child CID, you can also give the user access to other child CIDs. Specify this information for each CID you want to give the user access to:
 - a. Click Add CID.
 - b. Select a CID from the list.
 - c. Assign one or more roles. These roles only apply when the user is working in the associated CID.
 - d. Select one or more host groups for user access in this CID. For more info about FGA host access in parent and child CIDs, see [FGA for hosts and Flight Control](#).
10. Click Create user.

After creating a user account, if SSO isn't enabled in your environment, CrowdStrike sends an automated email to the user, prompting them to create a Falcon password and configure MFA. If SSO is enabled, CrowdStrike doesn't send an automated email to the user.

Viewing the users list

The [User management](#) page ([Host setup and management > Falcon users > User management](#)) lists all users in your organization and provides tools to create and manage user identities. Most tasks that pertain to users are performed from this page.

Falcon Management

- CID filter (FCTL parent CID only): Filter by CID to view users who are homed in or have access to a specific CID and see each user's assigned roles in the selected CID
- Search: Find users by email
- Export: Export user data to a [User details report](#)
- User email: The user's email address used to sign in to Falcon
- User name: The user's first and last names
- Home CID (FCTL parent CID only): The name of the user's home CID
- Roles:
 - Standalone CIDs and FCTL child CIDs: The roles assigned to each user.
 - FCTL parent CIDs: When viewing All CIDs, the user's assigned roles in their Home CID display. When filtering the users list by CID, the user's roles in the selected CID display.
- Account created*: The date and time the user's account was created
- Last login*: The date and time that the user last logged in to Falcon. Last login is not provided if a user has never logged in.
- Open menu  : Lists options to Open details panel, View details page, Reset MFA, Reset password, and Delete user
- Sort: By default, the users list is sorted alphabetically by User email. Reorder the list by clicking any column header with an arrow beside its name. A single click sorts in ascending order, and a second click sorts in descending order. The single arrow indicates which column is being used for sorting, and the arrow direction indicates the order (ascending or descending).

*Note: Account created dates preceding February 1, 2016 and Last login dates before September 1, 2021 might not be available for some users.

Viewing the User details page

The User details page provides detailed info about a specific user and tools to manage their identity.

To open the User details page, select View user details from a user's Open menu  on the [Host setup and management > Falcon users > User management](#) page or at the bottom of the details panel.

- User summary: View the user email address, User name, Home CID (FCTL only), Account created date and time, Last login date and time.

Note:

- Account created dates preceding February 1, 2016 and Last login dates before September 1, 2021 might not be available for some users.
- Last login is not provided if a user has never logged in.
- Edit user info: Make changes to the user's first and last name
- Open menu  : Additional actions to Reset MFA, Reset password, or Delete user
- Roles:
 - Standalone CIDs and FCTL child CIDs: See all roles currently assigned to the user, assign new roles, and remove existing roles
 - FCTL parent CIDs: See the CIDs the user has access to, view and manage the roles assigned in each CID, and grant access to additional CIDs
 - Temporary roles: See all temporary roles currently assigned to the user and when the temporary role expires.
- User groups: In FCTL users whose home CID is the parent CID, assign, view, and manage the person's user groups.

Manage a user's access

You can manage these facets of an existing user's Falcon console access in their user account:

- User roles: Each user is assigned at least one non-temporary role when their user account is created. You can add and remove roles for an existing user account. When a user is assigned a new role, it takes effect when the page is refreshed or the next time the user logs in.

For more info about roles and permissions, see [Role Management](#).

- Host groups: Each user can optionally be assigned one or more host groups for fine-grained access (FGA) when their user account is created. You can add and remove host groups for an existing user account. For more info about host groups, see [Managing host groups](#).
- Access scopes: Each user can optionally be assigned one or more access scopes for fine-grained access (FGA) to detections and advanced event search data. You can add access scopes when their user account is created and add or remove access scopes for an existing user account.

For more info about FGA, see [Controlling access to data with FGA](#).

Update user access

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Find the desired user account, click Actions  > View details page.
3. If you are managing user access in a Flight Control parent CID, on the Access per CID tab, expand the CID where you want to manage access.
4. Manage the user's roles:

Falcon Management

- Assign a role
 - Click Assign roles.
 - Select one or more roles, then click Assign.
- Assign a temporary role
 - Click Assign temporary roles.
 - Select one or more roles, set the temporary role duration, and then click Assign.
- To reduce or extend the duration of a temporary role, assign the same temporary role and set a new duration.
- To remove an assigned role, click Remove. After being removed, the user loses access to the role and its associated capabilities.

Note: A user is required to have at least one non-temporary role in each assigned CID. In the home CID, a role cannot be removed if it's the only role assigned. In CIDs that are directly assigned outside of the home CID, if you remove the last role assigned to the user, they lose access to the CID.

5. Manage the user's host groups:

- To assign host groups, click Assign host groups, select one or more host groups, then click Assign.

Note: If a user is currently assigned a value of All hosts, you must remove that value before you can narrow access to one or more specific host groups. However, you don't have to remove host group values if you want to update a user with access to All hosts. When you select All hosts, any existing host group assignments are saved. If you remove All hosts, any host group assignments the user had before being assigned All hosts are restored.
- To remove an assigned host group, click Remove. After being removed, the user loses access to hosts that belong to the host group, unless a host belongs to another host group the user is assigned.

6. Manage the user's access scopes:

- To assign access scopes, click Assign access scopes, select one or more access scopes, then click Save selection.
- To remove an assigned access scopes, click Remove. After the access scope is removed, the user has access to the data that was previously filtered out.

Update host group assignments using bulk actions

To add or remove host groups from more than one user account at once, use bulk actions:

1. Go to Host setup and management > Falcon users > User management .
2. Select applicable users.
3. Click Bulk action and select whether you want to assign or remove host groups from the selected user accounts.
 - Assign host groups: Select the host groups you want to assign to the selected users and click Assign host groups.
 - Remove host groups: Select the host groups you want to remove from the selected users and click Remove host groups.

Note: If you select a value of All hosts to remove from the selected users, only that value is removed, all other host group assignments remain. If you remove All hosts, any host group assignments the user had before being assigned All hosts are restored.

Delete users

To delete users, you must have an administrative role for your Falcon subscription, such as Falcon Administrator or Falcon Intel Admin. The Falcon Security Lead can reset user passwords and MFA, but cannot manage users or user roles.

For the user you want to delete, go to Host setup and management > Falcon users > User management , click Open menu  and select Delete user.

1. Go to Host setup and management > Falcon users > User management . You can also delete a user from the Open menu  inside the user info panel.
2. Next to the user who you want to delete, click Open menu  and select Delete user.
3. At the confirmation prompt, click Delete.

Managing access for user accounts

You can manage these aspects of user access for existing user accounts:

- Update a user's roles
- Update a user's host group assignments
- Update a user's cloud group assignments
- Update a user's access scope assignments
- Reset user passwords
- Reset Falcon MFA

You can also use bulk actions to manage these aspects of access for multiple users at once:

- Update host group assignments using bulk actions
- Update cloud group assignments using bulk actions

Find and review users

The User management page lists all users in your organization and provides tools to create and manage user identities. The list includes user info such as email address, roles, host groups and cloud groups, account created, and last login. Most tasks that pertain to users are performed from this page.

1. Go to Host setup and management > Falcon users > User management .
2. Use the search function, filters, and sorting to find users in the list.
3. Click a row to open the info panel for that user. The info panel includes Access per CID info and links to pages where you can review and edit names, roles, host groups, and cloud groups.
4. Click View details page for more info about roles and groups. You can edit the username and assign and remove roles, host groups, and cloud groups.

Notes:

- Account created dates preceding February 1, 2016 and Last login dates before September 1, 2021 might not be available for some users.
- Last login is not provided if a user has never logged in.
- You can filter the user list to show users that are assigned temporary roles.

Falcon Management

Update a user's roles

Each user is assigned at least one role when their user account is created. You can add roles for an existing user account. When a user is assigned a new role, it takes effect when the page is refreshed or the next time the user logs in. When you remove roles for an existing user account, the user loses access to the role and its associated capabilities.

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Find the user account you want to assign roles to, click Open menu  and select View details page.
3. If you are managing user access in a Flight Control parent CID, on the Access per CID tab, expand the CID where you want to manage access.
4. Manage the user's roles:
 - o To assign a role, click Assign roles, select one or more roles, then click Assign.
 - o To assign a temporary role, click Assign temporary roles, select one or more roles, set the temporary role duration, and then click Assign.
 - o To extend or shorten the duration of a temporary role, assign the same temporary role and set a new duration.
 - o To delete a role or a temporary role, find the assigned role you want to remove and then click Remove.

Tip: If you want to replace a role with a temporary one, remove the role, and then add the same role as a temporary role.

Update a user's host group assignments

Each user can optionally be assigned one or more host groups for fine-grained access (FGA) when their user account is created. You can add host groups for an existing user account. When you remove host groups from an existing user account, the user loses access to hosts that belong to that host group, unless a host belongs to another host group the user is assigned.

Note: If a user is currently assigned a value of All hosts, you must remove that value before you can narrow access to one or more specific host groups. However, you don't have to remove host group values if you want to update a user with access to All hosts. When you select All hosts, any existing host group assignments are saved. If you remove All hosts, any host group assignments the user had before being assigned All hosts are restored.

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Find the user account you want to assign a host group to, click Open menu and select View details page.
3. If you are managing user access in a Flight Control parent CID, on the Access per CID tab, expand the CID where you want to manage access.
4. Manage the user's host groups:
 - o To assign a host group, click Assign host groups, select one or more host groups, then click Assign.
 - o To delete a host group, find the host group you want to remove and click Remove.

Update host group assignments using bulk actions

To add or remove host groups from more than one user account at once, use bulk actions:

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Select applicable users.
3. Click Bulk action and select whether you want to assign or remove host groups from the selected user accounts.
 - o Assign host groups: Select the host groups you want to assign to the selected users and click Assign host groups.
 - o Remove host groups: Select the host groups you want to remove from the selected users and click Remove host groups.

Note: If you select a value of All hosts to remove from the selected users, only that value is removed, all other host group assignments remain. If you remove All hosts, any host group assignments the user had before being assigned All hosts are restored

Update a user's cloud group assignments

Each user with the proper subscription can optionally be assigned one or more cloud groups for FGA when their user account is created. You can assign more cloud groups to an existing user account. Cloud groups can be removed from an existing user account.

Note: If a user is currently assigned a value of All cloud groups, you must remove that value before you can narrow access to one or more specific cloud groups. However, you don't have to remove cloud group values if you want to update a user with access to All cloud groups. When you select All cloud groups, any existing cloud group assignments are saved. If you remove All cloud groups, any cloud group assignments the user had before being assigned All cloud groups are restored.

1. Go to [Host setup and management > Falcon users > User management](#) .
2. For the user you want to assign the cloud group to, click Open menu  and select View details page.
3. If you are managing user access in a Flight Control parent CID, on the Access per CID tab, expand the CID where you want to manage access.
4. Manage the user's cloud groups:
 - o To assign a cloud group, click Assign cloud groups, select the cloud groups you want this user associated with, then click Assign cloud groups.
 - o To delete a cloud group, find the cloud group you want to remove and click Remove.

Update cloud group assignments using bulk actions

To add or remove cloud groups from more than one user account at once, use bulk actions:

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Select applicable users.

Falcon Management

3. Click Bulk action and select whether you want to assign or remove cloud groups from the selected user accounts.

- Assign cloud groups: Select the cloud groups you want to assign to the selected users and click Assign cloud groups.
- Remove cloud groups: Select the cloud groups you want to remove from the selected users and click Remove cloud groups.

Note: If you select a value of All cloud groups to remove from the selected users, only that value is removed, all other cloud group assignments remain. If you remove All cloud groups, any cloud group assignments the user had before being assigned All cloud groups are restored.

Update a user's access scope assignments

Each user can optionally be assigned one or more access scopes for fine-grained access (FGA) to detections and advanced event search data. You can add access scopes when their user account is created and add or remove access scopes for an existing user account. For more info, see [Access Scopes](#).

1. Go to [Host setup and management > Falcon users > User management](#).
2. Find the user account you want to assign an access scope to, click Open menu  and select View details page.
3. Manage the user's access scopes:
 - To assign an access scope, click Assign access scopes, select one or more access scopes, then click Save selection.
 - To delete an access scope, find the access scope you want to remove and click Remove.

Reset user passwords

If SSO isn't enabled in your environment, users can reset their own passwords from the Falcon login page or from their Falcon User Profile page. If SSO is enabled, users cannot reset their own passwords.

To reset another user's password, you must have an administrative role for your Falcon subscription, such as Falcon Administrator or Falcon Intel Admin. The Falcon Security Lead can reset user passwords and MFA, but cannot manage users or user roles.

Note: If SSO is enabled in your environment, this functionality is not available. Reset passwords in your IdP, not in the Falcon console.

1. Go to [Host setup and management > Falcon users > User management](#).
- You can also reset a user's password from Open menu  inside the User details.
2. Next to the user whose password you want to reset, click Open menu  and select Reset Password.
3. At the confirmation prompt, click Send request. CrowdStrike sends an automated email to the user, prompting them to reset their Falcon password.

Note: When you reset a user's password, that user is logged out of all active sessions, requiring a new log in.

Password requirements

When changing or resetting a password, the new password must meet these requirements:

- Minimum length of 12 characters
- No more than 2 repeated characters in a row
- Contains at least 1 character from each of these sets:
 - Numbers
 - Uppercase letters
 - Lowercase letters
 - Special characters:
~ ! @ # ? \$ % ^ & * () - _ = + [] { } | ; : , . { } / ?
- Doesn't contain sequences of 4 or more characters from these ordered sets:
 - Numeric, such as 0123 or 6789
 - Alphabetical, such as abcd or opqr
 - Keyboard layout, such as qwer or asdf
- Can't be one of the user's 5 previously used passwords

Reset Falcon MFA

You can reset multi-factor authentication (MFA) for individual users from the User management page or inside the User details.

Note: Users can not reset their own MFA. If you need to reset your MFA, contact your account administrator.

Resetting MFA applies to:

- Users who log in to Falcon with MFA: The next time the user logs in they will be prompted to configure Falcon MFA.
- Users who log in to Falcon with a third-party SSO and use Real Time Response identity verification: The next time the user attempts an MFA-enforced RTR action they will be prompted to configure Falcon MFA for RTR.
- Users who log in to Falcon with MFA and use Real Time Response identity verification: The next time the user logs in or attempts an MFA-enforced RTR action they will be prompted to configure Falcon MFA.

Note: MFA resets do not apply to Single Sign-On (SSO) for Falcon. If SSO is enabled in your environment, configure and manage those settings in your IdP, not in Falcon.

Falcon Management

1. Go to [Host setup and management > Falcon users > User management](#) .

You can also reset MFA from the Open menu  inside the User details.

2. Next to the user whose MFA you want to reset, click Open menu  and select [Reset MFA](#).
3. At the confirmation prompt, click [Send request](#). The user is prompted to configure Falcon MFA the next time they log in or attempt an MFA-enforced RTR action.

Generating a User details report

Export and download a CSV or JSON file of your user data. The User details report includes the following information for each user:

- Exports from standalone CIDs and FCTL child CIDs:
 - First name
 - Last name
 - Email address
 - Roles
 - Account created
 - Last login
 - User UUIDs (JSON format only)
 - Factors
- Exports from FCTL parent CIDs: Include all fields from standalone CIDs and FCTL child CIDs user details report plus:
 - CID
 - CID roles
 - CID roles expire at (Temporary roles only)
 - Home CID

You can choose to export all users or apply search, filter, and sort options to create a custom list with a subset of users. The exported file includes all pages of users that match the filter criteria and reflects the exact ordering from the result list in Falcon.

1. On [Host setup and management > Falcon users > User management](#) , click [Export users](#).
2. Choose the file format for your report (CSV or JSON).
3. When the report is ready, click [Download](#).

After a report is generated, the file is available for download for 24 hours.

Role Management

View and manage Falcon access control settings for your Falcon console users.

Role Management

View and manage Falcon access control settings for your Falcon console users.

Requirements

Role: Falcon Administrator

Understanding Falcon role-based access control

Falcon uses role-based access control (RBAC) to determine the access settings of each Falcon console user. These elements are the foundation for access in the Falcon console:

- **Permission:** Access to perform a specific action on an object, such as [View Firewall policies](#) or [Modify mobile policies](#). Permissions are not assigned to users directly, they are only granted by being enabled in roles that are assigned to users. Permissions are organized into permission groups in the Falcon console, such as [Prevention Policies](#) or [Host Management](#).
- **Role:** A logical collection of permissions enabled based on the workflow of similar users, such as [Falcon Analyst](#) or [Endpoint Manager](#). Roles are assigned to users and define the permissions these users have access to. There are 2 role types:
 - **Default roles:** Roles created by CrowdStrike to handle most user flows. These roles are provided by default and can't be updated.
 - **Custom roles:** Roles created by your organization to refine permissions only for users in your CID.
 - **Temporary roles:** Default and custom roles that are assigned to users for a limited period of time to control access to sensitive information and escalated privileges.

Multiple role assignments and access control

A user gains permissions by being assigned a role that has those permissions enabled. A user is granted all permissions enabled by all of the roles they are assigned. Roles do not revoke permissions, they only grant permissions. Therefore, permissions can only be denied by removing from the user the role that grants access.

Falcon Management

The User management page prevents you from assigning a role to someone who already has that role. The user role API permits assigning duplicate roles. Roles are additive. When a temporary role expires and is revoked, if a user has a duplicate non-temporary role, access to that role is maintained. For more info about the user roles API, see [Grant or revoke user roles](#).

Viewing role details

You can view all active roles in your CID in the Falcon console. Go to [Host setup and management > Falcon users > Roles and permissions](#). Each role is listed with a description and this overview info:

- **Role type:** Identifies the role as a default role or a custom role
- **Permissions:** Number of permissions enabled for the role
- **Users:** Number of users assigned the role
- **Groups:** For Flight Control, the number of user groups and CID groups assigned the role

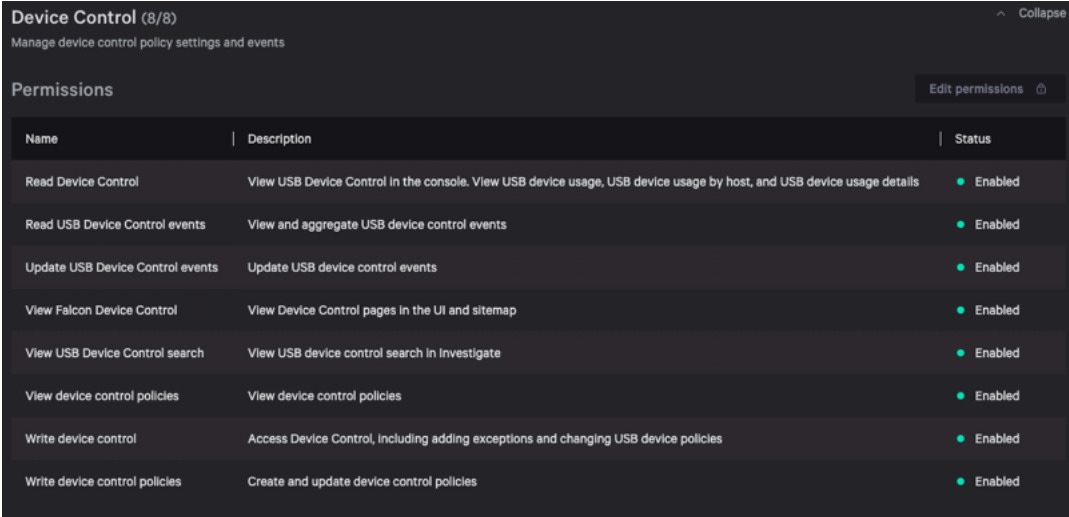
To see details about a role, click the actions menu  and select [View role details](#).

Role permissions

To view all permissions enabled for a role, go to [Host setup and management > Falcon users > Roles and permissions](#), click the actions menu  for the role, and select [View role details](#).

On the details page for the role, click the **Permissions** tab. All Falcon permissions are listed by permission group. Each permission indicates if it is enabled or disabled. A status of **Enabled** means users assigned this role have access to the permission, such as [View FileVantage changes](#).

You can collapse permission groups or use one of these filters:



Name	Description	Status
Read Device Control	View USB Device Control in the console. View USB device usage, USB device usage by host, and USB device usage details	Enabled
Read USB Device Control events	View and aggregate USB device control events	Enabled
Update USB Device Control events	Update USB device control events	Enabled
View Falcon Device Control	View Device Control pages in the UI and sitemap	Enabled
View USB Device Control search	View USB device control search in Investigate	Enabled
View device control policies	View device control policies	Enabled
Write device control	Access Device Control, including adding exceptions and changing USB device policies	Enabled
Write device control policies	Create and update device control policies	Enabled

- **Permission group:** Select one or more permission groups that you want to see and click [Apply](#). Each group in the list shows how many permissions are in the group and how many of the total are currently enabled for the role.
- **Permission status:** Select to show either all **Enabled** or all **Disabled** permissions, then click [Apply](#).

You can update permissions for custom roles, but not for default roles. See [Edit custom role permissions](#).

Role users and groups

To view users and groups currently assigned a role, go to [Host setup and management > Falcon users > Roles and permissions](#), click the actions menu  for the role, and select [View role details](#).

On the details page for the role, click one of these tabs to view info:

Falcon Management

- Users: Shows all users currently assigned the role. Each user record includes their name, email address, and a list of all roles they are assigned.

You can perform these actions:

- To assign the role to one or more additional users, click Assign to more users, search for each user to add to the list of users, and then click Assign role.
- To remove the role from the user, click the actions menu  and select Remove role from user.
- To go to the user record and see more details, click the actions menu  and select View user details.

For more info, see [Managing users](#).

- Groups: For environments with Flight Control or a multi-CID account, this tab shows all of the user groups and CID groups currently assigned the role. Each user and CID group record includes the user and CID group name, and a list of roles assigned to the user and CID group.

You can perform these actions:

- To go to the user groups page and manage all user groups, click Go to user groups.
- To go to a specific user group or CID group record and see more details, click the actions menu  and select View user group details or View CID group details.

For more info, see [Falcon Flight Control and Multi-CID Support](#).

Managing custom roles

We recommend using the Falcon default roles whenever possible to meet your access control needs. Default roles are maintained and supported by CrowdStrike and are updated with new permissions for new features.

If the default Falcon roles don't meet a specific business need, you can create a custom role and define permissions so your users have only the access you want them to have.

Important: Custom roles that you create in your CID are not supported or maintained by CrowdStrike. These custom roles are the responsibility of your organization to create, maintain, and support, including adding new permissions for new Falcon features that are released. Additionally, our Support team cannot use custom roles to verify that you're authorized to request changes on an account.

Best practice: duplicate default roles

We strongly recommend you create a new custom role by duplicating a default Falcon role and modifying it to meet your needs. It is much easier and safer to duplicate a role and then add or remove permissions than to create a new role with no existing permissions. For examples of creating a custom role by duplicating a default role, see [Custom role examples](#).

Important: Always test and verify the behavior of custom roles before assigning to users in your production environment.

Custom role examples

These custom role examples show how an existing default Falcon role is duplicated to create a new custom role. The new custom role is then modified to restrict access and meet business needs.

In this scenario, an organization has IT personnel who make sure employees have user accounts in necessary systems. This organization doesn't need these IT personnel to perform any other actions in the console and doesn't want regular console users to have access to employee user accounts. This organization can accommodate these business needs by creating these custom roles:

- An admin role that is similar to the default role Falcon Administrator but doesn't have access to create and manage users.
- An admin role that only includes permissions to create and manage users and doesn't have access to other permissions.

Example: Admin role that can't create users

To create an admin role that is similar to the default Falcon Administrator role that can't create users:

1. Create a new custom role that is a duplicate of the Falcon Administrator role.
2. In the new custom role, locate the Manage All Users permission group and disable all except these permissions:
 - View User Details
 - View Users

The new custom role has all of the permissions that the Falcon Administrator role has except creating and managing users. Users assigned this role can view user accounts in the console, but cannot create or manage them.

For more info about creating custom roles, see [Creating custom roles](#).

For more info about managing custom role permissions, see [Edit custom role permissions](#).

Example: Admin role that can only create users

To create an admin role that can only create users:

1. Create a new custom role that is a duplicate of the Falcon Administrator role.
2. In the new custom role, ensure all permissions in these permission groups are enabled:
 - Manage All Users
 - Role Management
 - Custom User Roles

Falcon Management

3. Disable all permissions in all other permission groups.

The new custom role has permissions to only create and manage users.

For more info about creating custom roles, see [Creating custom roles](#).

For more info about managing custom role permissions, see [Edit custom role permissions](#).

Custom roles and Multi-CID environments

Unlike default roles, custom roles are specific to the CID in which they are created. For Flight Control multi-CID environments, custom roles must be created and assigned in the home CID of the user. You can't assign a custom role to a user in a CID that is not their home CID.

Custom roles that are defined and assigned in a parent CID to users for whom the parent CID is their home CID also apply to those users working in child CIDs through default CID groups or user groups.

For more info, see [Flight Control access management](#).

For more info about user management, see [User Management](#).

Creating custom roles

When creating a custom role, we strongly recommend duplicating a default Falcon role and modifying it to meet your needs.

Important: Always test and verify the behavior of custom roles before assigning to users in your production environment.

Recommended: create a custom role from a duplicate

To create a new custom role using a duplicate of an existing role:

1. Duplicate an existing role using one of these methods:
 - On the Roles and permissions page, click the actions menu  of the role you want to duplicate and click Duplicate role.
 - On the role details page of the role you want to duplicate, click Duplicate role.
2. Specify a role name and description, then click Duplicate role.
3. Specify role permissions. See [Edit custom role permissions](#).
4. Verify the behavior of the custom role in a test environment or with a test user.
5. When the role is verified, assign it to users. See [Role users and groups](#).

Create a custom role

When creating a custom role, we strongly recommend duplicating a default Falcon role and modifying it to meet your needs. See [Recommended: creating a custom role from a duplicate](#).

To create a custom role that is not a duplicate of an existing role:

1. Go to Host setup and management > Falcon users > Roles and permissions and click Create role.
2. Specify a role name and description, then click Create role.
3. Specify role permissions. See [Edit custom role permissions](#).

Note: Every custom role is granted, by default, the minimal permissions required to login to the Falcon console. These permissions are not visible on the Permissions tab.

4. Verify the behavior of the custom role in a test environment or with a test user.
5. When the role is verified, assign it to users. See [Role users and groups](#).

Edit custom role permissions

You can edit permissions for custom roles to restrict or expand access to information and tasks in the Falcon console for users who are assigned that role.

To update permissions for a custom role:

1. Go to Host setup and management > Falcon users > Roles and permissions, click the actions menu  for the role, and select View role details.
2. On the Permissions tab of the role details page for a custom role, locate the permission group with permissions you want to edit and click Edit permissions.
3. Select the check box of permissions you want to enable and clear the check box of permissions you want to disable, then click Save.

Note: Some permissions are dependent on other permissions. If you try to enable or disable a permission that has a dependency on one or more additional permissions, a message prompts you to approve adding or removing the dependent permissions before you can enable or disable the permission with the dependency.

Note: You can't edit permissions for default roles.

Delete a custom role

Custom roles that are currently in use can't be deleted. You must first remove the role from all users it is currently assigned to. See [Role users and groups](#).

Falcon Management

To delete a custom role, perform one of these actions:

- Go to [Host setup and management > Falcon users > Roles and permissions](#), click the actions menu  for the role, and click [Delete role](#).
- On the [role details](#) page of the role you want to delete, click [Delete role](#).

Note: You can't delete default roles.

Best practice: Real Time Response roles and permissions

Be very careful when including Real Time Response (RTR) permissions in custom roles. These permissions can potentially be disruptive and access should only be permitted to users who understand and accept the associated responsibilities.

For more info about RTR roles and permissions, see [Real Time Responder roles](#).

Default Roles Reference

Look up the key capabilities of Falcons default roles.

Cross-subscription default roles

These default roles represent various types of access and functionality that can be applied to any Falcon product subscription.

For complete details on one or more of these roles, including the permissions they include, go to [Host setup and management > Falcon users > Roles and permissions](#), click the actions menu for the role, and select [View role details](#). For more info, see [Role Management](#).

Falcon Management

- **Falcon Console Guest:** (View-only) View documentation and your user profile. Visit the CrowdStrike Customer Center to review knowledge base articles, read and subscribe to release notes and tech alerts, and use the chatbot for automated help.

- **Falcon Administrator:** Access to all functionality in both the Falcon console and Kestrel, with the exception of certain Real Time Response (RTR) capabilities.

For more info, see the role descriptions for each Falcon subscription or app. For more info about RTR roles, see the Requirements section of Real Time Response and Network Containment.

- **Falcon Investigator:** Manage detections, search for events, and view exclusions. View data about assets, accounts, and applications in asset management. View Falcon Sandbox submissions and reports. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. Manage Identity Protection insights, incidents, reports, and threat hunter. View FileVantage file integrity policies, rule groups, and activity. Create and run on-demand scans from the Falcon console.
- **Falcon Analyst:** Manage detections and quarantined files and view exclusions and host management. Create and manage scheduled searches and view and download the results. View Falcon Sandbox submissions and reports. View FileVantage file integrity policies, rule groups, and activity. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. View Falcon icon policies.
- **Falcon Analyst - Read Only:** View detections and exclusions and search for events. View all Identity Protection info. View FileVantage file integrity policies, rule groups, and activity. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. View data about assets, accounts, and applications in asset management.
- **Falcon Security Lead:** Manage detections, manage quarantined files, contain hosts, search for events, reset users' credentials, and view exclusions. View data about assets, accounts, and applications in asset management.
- **Workflow Author:** Create, duplicate, and edit workflows. Re-execute a failed workflow execution. This role doesn't grant basic Falcon console access. Users assigned this role must have at least one other role assigned to access the Falcon console. Users assigned this role can't include RTR actions in workflows or re-execute a failed workflow that contains RTR actions unless they are also assigned the Real Time Responder - Administrator role.
- **Dashboard Admin:** Create, edit, manage, and delete [dashboards](#). Create and edit shared [tables](#). This role does not grant basic Falcon console access. Users assigned this role must have at least one other role assigned to access the Falcon console.
- **Scheduled Report Admin** can assign and revoke the Scheduled Report Analyst role, create scheduled reports, view and manage any scheduled report in the CID, and view, download, and delete any generated report in the CID.
- **Scheduled Report Analyst** can only access the Scheduled reports page and view and download generated reports of scheduled reports that have been specifically shared with them. You can assign this role to members of your team who need to access scheduled reports but do not need any other Falcon access. For example, you might assign this role to IT staff who need to access periodic reporting metrics to stay on top of vulnerabilities.
- **Prevention Policy Manager:** Create, edit, and delete prevention policies. Turn select prevention policy settings on and off. Users with this role can also view dashboards, host management, detections management, file exclusions, sensor update policies, and audit logs.
- **Endpoint Manager:** Manage sensor deployment and maintain sensor configuration and update policies. Create and edit host groups. Download Forensics app.
- **Detections Exceptions Manager:** Add, edit, and manage custom IOCs, ML exclusions, IOA exclusions, and sensor visibility exclusions.
- **Event Viewer:** Search for events. View data about assets, accounts, and applications in asset management.
- **Desktop Support Analyst:** Install sensor, troubleshoot, view manuals, and access documentation about products' functions and restrictions. View Falcon icon policies.
- **Help Desk Analyst:** View detections, host management, installation tokens, prevention policies, file exclusions, sensor update policies, and dashboards. View Falcon icon policies.

Note: Although this role allows users to view host information in host management, users must also be assigned a role that gives them access to user information in order for them to see details in the User Info section of a host's details.

- **MSSP Co-Managed NG-SIEM Admin:** This role is for Managed Security Service Providers (MSSPs) in customer CIDs where Falcon Complete manages first-party endpoint, identity, or cloud detections and the MSSP manages third-party detections in Next-Gen SIEM. It allows users to view detections managed by Falcon Complete while managing Next-Gen SIEM detections. This role can:
 - Access customer data needed for SIEM integration
 - Access event data streams
 - Access logs and events
 - Configure event types for streaming
 - Configure SIEM integration settings
 - Create and manage SIEM connectors
 - Create new users
 - Manage SIEM configurations for assigned customers
 - Monitor event delivery status
 - View and modify SIEM streaming settings
 - View assigned customer environments
 - View configuration settings
 - View detection data
- **Kestrel Administrator:** Access Kestrel and use all Kestrel features. Give other users access to Kestrel.
- **Kestrel User:** Access Kestrel and use all Kestrel features.

Default roles by subscription

These sections show Falcon default roles available to each subscription.

For complete details on one or more of these roles, including the permissions they include, go to [Host setup and management > Falcon users > Roles and permissions](#), click the actions menu for the role, and select [View role details](#). For more info, see [Manage a user's access](#).

Falcon Management

Roles for Charlotte AI

- Falcon Administrator: Grant Charlotte AI roles and can access all of Charlotte AI
- Charlotte AI Analyst: Send prompts to Charlotte AI, view own past conversations
- Charlotte AI Auditor: View the Charlotte AI audit log and see all past prompts and response
- Charlotte AI Promptbook Manager: View and edit Organization promptbooks
- Charlotte AI Usage Monitor: View the Credit Monitoring dashboard

Table 1. Charlotte AI Roles

	Falcon Administrator	Charlotte AI Analyst	Charlotte AI Auditor	Charlotte AI Promptbook Manager	Charlotte AI Usage Monitor
Send prompts to Charlotte AI	Yes	Yes	No	No	No
View own past conversations	Yes	Yes	Not applicable	Not applicable	Not applicable
View all past conversations in Charlotte AI audit log	Yes	No	Yes	No	No
Grant Charlotte AI roles	Yes	No	No	No	No
View all promptbooks	Yes	No	Yes	Yes	No
Create a promptbook	Yes	Yes	No	Yes	No
View Credit Monitoring dashboard	Yes	No	No	No	Yes

Roles for Cloud Security

- Cloud Security Manager:
 - This role provides full access to all of Falcon Cloud Security.
 - View all cloud and Kubernetes and containers assets in the Falcon console.
 - Manage protection policies and roles.
 - Provision and deprovision public cloud accounts. This role must obtain the API and client keys from a Falcon Administrator to successfully register a cloud account.
- Kubernetes and Containers Manager:
 - View Kubernetes and containers in the Falcon console.
 - Provision and deprovision public cloud accounts for discovering Kubernetes clusters. This role must obtain the API and client keys from a Falcon Administrator to successfully register a cloud account.
- CSPM Manager:
 - View cloud assets in the Falcon console.
 - Manage cloud security posture management policies and roles.
 - Provision and deprovision public cloud accounts for discovering cloud assets. This role must obtain the API and client keys from a Falcon Administrator to successfully register a cloud account.
- CSPM Misconfiguration Viewer:
 - View cloud asset misconfigurations in the Falcon console.
- Cloud Compliance Viewer:
 - View compliance details about cloud assets in the Falcon console.
- Image Viewer:
 - View details about image vulnerabilities, image assessment policies, and registry connections in the Falcon console.
 - This role was formerly named Falcon Container Image Viewer.

Deprecated Cloud Security roles

The following roles are deprecated. They are still available in the Falcon console, but to maintain access to new Falcon Cloud Security features, we encourage you to use other roles. Deprecated roles may not be supported for use with new features.

- CSPM Analyst
- CSPM Read-Only Analyst
- Falcon Container Image Admin
- Kubernetes Protection Admin
- Kubernetes Protection Analyst
- Kubernetes Protection Read-Only Analyst

This table provides suggested replacements for the deprecated roles:

Deprecated Role	Suggested Default Role	Suggested Custom Role
CSPM Analyst (deprecated)	CSPM Manager Note: This role includes Cloud Security Registration permissions that are not enabled for CSPM Analyst.	Create a custom role based on the CSPM Misconfiguration Viewer role and adding IOAs permissions.
CSPM Read-Only Analyst (deprecated)	CSPM Misconfiguration Viewer	Create a custom role based on the CSPM Misconfiguration Viewer role and adding IOAs permissions.

Falcon Management

Falcon Container Image Admin (deprecated)	Kubernetes and Containers Manager	Create a custom role based on the Image Viewer role and add write access.
Kubernetes Protection Admin (deprecated)	Kubernetes and Containers Manager	Create a custom role with write access for the Kubernetes misconfigurations page.
Kubernetes Protection Analyst (deprecated)	Image Viewer	Create a custom role with write access for the Kubernetes misconfigurations page.
Kubernetes Protection Read-Only Analyst (deprecated)	Image Viewer	Create a read-only custom role for the Kubernetes misconfigurations page.

To check whether deprecated roles are in use and migrate users to new roles:

1. In the Falcon console, go to [Host setup and management](#) > [Falcon users](#) > [Roles and permissions](#).
2. For each of the deprecated roles, check the Users column to see how many users are assigned to the role.
3. If there are users assigned:
 - a. Click Open menu , select View role details, and then go to the Users tab to see a list of users assigned to the role.
 - b. Copy the list of users.
 - c. Assign the users to a new default or custom role. For instructions on how to create custom roles, see [Managing custom roles](#).

Roles for Counter Adversary Operations

	Falcon Admin	Intel Admin	Intel Basic Analyst	Intel All Analyst ¹	Intel Targeted Analyst ¹	Intel eCrime Analyst ¹	Intel Malware Submitter ¹	Falcon Investigator
See Falcon Sandbox submissions and reports	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Submit samples to Falcon Sandbox	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Submit malware samples to the Falcon Intelligence team	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Use MalQuery Search, Hunt, and Monitor	Yes	No	No	No	No	No	No	No
Grant the MalQuery user role to others	Yes	No, but can revoke both MalQuery user roles	No	No	No	No	No	No
Access Adversaries info	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Read release notes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Grant Intel type roles to others	Yes	Yes	No	No	No	No	No	No
Read eCrime	Yes	Yes	No	Yes	No	Yes	No	No

Falcon Management

	Falcon Admin	Intel Admin	Intel Basic Analyst	Intel All Analyst ¹	Intel Targeted Analyst ¹	Intel eCrime Analyst ¹	Intel Malware Submitter ¹	Falcon Investigator
reports, alerts, and feeds								
Manage Intel notifications	Yes	Yes	No	Yes	Yes	Yes	No	No
Read Targeted reports, alerts, and feeds	Yes	Yes	No	Yes	Yes	No	No	No
Read Tailored Intelligence rules and hits	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Create Tailored Intelligence rules	Yes	No	No	No	No	No	No	No

¹ - Falcon Intelligence Premium subscriptions only

The following roles require one of these subscriptions:

- Falcon Adversary Intelligence
- Falcon Adversary Intelligence Premium
- Counter Adversary Elite

	Counter Adversary Elite Admin	Counter Adversary Elite Analyst	Adversary Intelligence Premium Admin	Adversary Intelligence Premium Analyst	Adversary Intelligence Premium Investigator
View threat landscape	Yes	Yes	Yes	Yes	Yes
Access intelligence dashboards	Yes	Yes	Yes	Yes	Yes
Access information about adversaries, malware families, and indicators	Yes	Yes	Yes	Yes	Yes
View vulnerability intelligence	Yes	Yes	Yes	Yes	Yes
Read intelligence reports and feeds	Yes	Yes	Yes	Yes	Yes
Submit samples to Sandbox and get reports	Yes	Yes	Yes	Yes	No
Submit malware samples and RFIs to the CrowdStrike Intelligence team	Yes	Yes	Yes	Yes	No

Falcon Management

	Counter Adversary Elite Admin	Counter Adversary Elite Analyst	Adversary Intelligence Premium Admin	Adversary Intelligence Premium Analyst	Adversary Intelligence Analyst
Access hunting library, intrusion digest, hunting reports, and threat hunting briefings	Yes	Yes	Yes	Yes	No
Use MalQuery Search, Hunt, and Monitor	Yes	Yes	Yes	Yes	No
Create Recon monitoring rules and view notifications	Yes	Yes	Yes	Yes	Yes
View Recon monitoring rules and notifications the user created and ones visible to all analysts	Yes	Yes	Yes	Yes	Yes
View all Recon monitoring rules and notifications	Yes	No	Yes	No	Yes
Create ownership verification tokens	Yes	Yes	Yes	Yes	Yes

Further reading

As an alternative to viewing the table of user roles for Falcon Intelligence, these sections repeat the same table info as sentences.

For Falcon Sandbox

- Users with these roles can view Falcon Sandbox submissions and reports, submit samples to Sandbox for analysis, and submit suspected malware to the Falcon Intelligence team.
 - Falcon Administrator
 - Intel Admin
 - Intel All Analyst¹
 - Intel Targeted Analyst¹
 - Intel eCrime Analyst¹
 - Intel Malware Submitter¹
- Users with these roles can view Falcon Sandbox submissions and reports, as well as submit samples to Sandbox for analysis, yet *cannot* submit suspected malware to the Falcon Intelligence team.
 - Intel Basic Analyst
- Users with these roles can view Falcon Sandbox submissions and reports:
 - Falcon Investigator
 - Falcon Security Lead
 - Falcon Analyst
 - Quarantine Manager
 - Real Time Responder - Read Only Analyst
 - Real Time Responder - Administrator
 - Real Time Responder - Active Responder

For Falcon Intelligence broadly

Falcon Management

- Intel Admin can access Adversaries, read release notes, manage users, submit malware, read all intel, and manage notifications.
- Intel All Analyst can access Adversaries, read release notes, submit malware, read all intel, and manage notifications.
- Intel Targeted Analyst can access Adversaries, read release notes, submit malware, read only Targeted intel, and manage notifications.
- Intel eCrime Analyst can access Adversaries, read release notes, submit malware, read only eCrime intel, and manage notifications.
- Intel Malware Submitter can access Adversaries, read release notes, and submit malware.
- Intel Basic Analyst can access Adversaries and read release notes.

For Falcon MalQuery

- MalQuery Admin can use all Falcon MalQuery features and give other users access to Falcon MalQuery.
- MalQuery User can use all Falcon MalQuery features.

Roles for SampleStore

These default roles can submit samples to SampleStore.

- Falcon Administrator
- Falcon Analyst
- Falcon Analyst - Read Only
- Falcon Investigator
- Falcon Security Lead
- Intel Admin
- Intel All Analyst
- Intel Basic Analyst
- Intel eCrime Analyst
- Intel Malware Submitter
- Intel Targeted Analyst
- Mobile Admin
- OverWatch Malware Submitter

Roles for Endpoint Detection and Response (EDR) scheduled searches

For info about roles for Next-Gen SIEM scheduled searches, see [Roles for Falcon Insight Next-Gen SIEM](#).

- Scheduled Report Admin and Falcon Administrator:
 - Can assign and revoke the Scheduled Report Analyst role.
 - Can create scheduled searches, and can edit and delete any scheduled search in the CID.
 - Can view, download, and delete any generated search result sets.
- Scheduled Report Analyst (included with Falcon Analyst):
 - Can create scheduled searches, and can edit and delete scheduled searches that they created.
 - Can view and download search result sets generated from scheduled searches that they created.

Roles for Falcon Application Security Posture Management (ASPM)

- ASPM Admin: Access and manage all ASPM capabilities including policy management, integrations, collectors and settings such as the ability to customize the risk score.
- ASPM Analyst: View all data and manage some capabilities such as violation status updates, creation of tickets and creation of automation rules.
- ASPM Read Only: View all data with no management capabilities.

	ASPM Admin	ASPM Analyst	ASPM Read Only
View dashboard	Yes	Yes	Yes
View inventory	Yes	Yes	Yes
View service details	Yes	Yes	Yes
View and export map	Yes	Yes	Yes
View and manage policies	Yes	No	No

Falcon Management

	ASPM Admin	ASPM Analyst	ASPM Read Only
View events	Yes	Yes	Yes
Create, run and save queries	Yes	Yes	Yes
View violations	Yes	Yes	Yes
Open tickets from violations	Yes	Yes	No
Change violation status	Yes	Yes	No
View and manage service classifiers	Yes	No	No
View and manage service actions	Yes	No	No
View automation rules and reports	Yes	Yes	Yes
Manage automation rules and reports	Yes	Yes	No
View integrations	Yes	Yes	No
Manage integrations	Yes	No	No
View collectors	Yes	Yes	No
Manage and run collectors	Yes	No	No
View risk customization settings	Yes	Yes	No
Manage risk customization settings	Yes	No	No
Create token for your user	Yes	Yes	Yes
Create token for others users	Yes	No	No
Manage existing tokens	Yes	Yes	No

Roles for Falcon Complete

Falcon Complete Hub

- Falcon Administrator: View items in the Falcon Complete hub. Act on suggested remediation actions.
- Falcon Complete Administrator: View items in the hub. Act on suggested remediation actions. View items in Falcon Flex dashboard.
- Falcon Analyst: View items in the hub.
- Falcon Analyst - Read only: View items in the hub.

Message Center

Message Center lets users exchange messages with the Falcon Complete and Falcon OverWatch teams about incidents and detections. These types of conversations are support cases with the Falcon Complete team. Message Center also lets users create and reply to CrowdStrike support cases for issues that are not related to Falcon Complete.

These roles can see and interact with Message Center if their organization has Falcon Complete:

Note: The Falcon Analyst - Read Only role can see Message Center but cannot create, contribute to, or manage cases.

Falcon Management

- Custom IOAs Manager
- Dashboard Admin
- Detections Exceptions Manager
- Device Control Manager
- Endpoint Manager
- Event Viewer
- Falcon Administrator
- Falcon Analyst
- Falcon Complete Contact Manager
- Falcon Investigator
- Falcon Recon Admin
- Falcon Recon Analyst
- Falcon Security Lead
- Firewall Manager
- Forensic Investigator
- Identity Protection Domain Administrator
- Identity Protection Policy Manager
- Intel Admin
- Intel All Analyst
- Intel Basic Analyst
- Intel eCrime Analyst
- Intel Malware Submitter
- Intel Targeted Analyst
- MalQuery Admin
- MalQuery User
- Mobile Admin
- Quarantine Manager
- Real Time Responder - Active Responder
- Real Time Responder - Administrator
- Real Time Responder - Read Only Analyst
- Vulnerability Manager

Roles for Falcon Data Protection

- Data Protection Admin: Can access all Falcon Data Protection features and functionality, including the ability to create, view, and manage policies, classifications, and rules.
- Data Protection Analyst: Can view all Falcon Data Protection policies, classifications, and rules.

Roles for Falcon Discover for IoT

- Falcon Administrator: Access all functionality across Discover for IoT. Grant and revoke Discover OT Operations roles.
- Discover OT Operations: Can view asset and application data in Discover for IoT. Can view and manage ICS collections.

	Falcon Administrator	Discover OT Operations
View Discover IoT applications data	Yes	Yes
View IoT hosts data	Yes	Yes
Cancel ongoing ICS asset collections	Yes	Yes
Create asset's collection schedule	Yes	Yes

Falcon Management

	Falcon Administrator	Discover OT Operations
Update schedule	Yes	Yes
View ICS asset collections	Yes	Yes
View ICS assets	Yes	Yes
View schedules	Yes	Yes

Roles for Falcon Exposure Management

- Falcon Administrator: Access all functionality across Falcon Exposure Management including asset management, vulnerability management, configuration assessment, external attack surface management, and granting and revoking roles.
- Exposure Management Manager: Access all functionality across Falcon Exposure Management including asset management, vulnerability management, configuration assessment, external attack surface management, attack path analysis, and granting and revoking roles.
- Attack Path Analyst: View attack paths. View risk overlays in the asset graph view. Must be combined with other roles.
- Risk Manager: View risk overlays in the asset graph view. Must be combined with other roles.

Roles for asset management

These roles are included in the Falcon Exposure Management and Falcon Discover subscriptions.

- Exposure Assets Admin: Access all functionality across asset management, grant and revoke Exposure Assets Analyst role
- These roles can view data about assets, accounts, and applications, and view reports and configurations:
 - Exposure Assets Analyst
 - Falcon Security Lead
 - Falcon Investigator
 - Falcon Analyst - Read Only
 - Event Viewer

	Falcon Administrator	Exposure Management Manager	Exposure Assets Admin	Exposure Assets Analyst	Falcon Security Lead	Falcon Investigator	Falcon Analyst - Read Only
View data about assets, accounts, and applications	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Update information about assets, including triage and manually assigning asset roles, criticality levels, and internet exposure	Yes	Yes	Yes	No	No	No	No
View risk overlays, badges, factors, and details in the asset graph view	Yes	Yes	Yes	No	No	No	No
Configure application groups	Yes	Yes	Yes	No	No	No	No
View application	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Falcon Management

	Falcon Administrator	Exposure Management Manager	Exposure Assets Admin	Exposure Assets Analyst	Falcon Security Lead	Falcon Investigator	Falcon Analyst
groups							
Configure passive discovery	Yes	Yes	Yes	No	No	No	No
View passive discovery configurations	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Configure active discovery through network scanning	Yes	Yes	No	No	No	No	No
Create and manage rules for dynamic asset criticality assignment	Yes	Yes	Yes	No	No	No	No
View asset criticality levels	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Set up third-party data ingestion	Yes	Yes	No	No	No	No	No
Set up Falcon Fusion SOAR workflows that update asset data Must be paired with the Workflow Author role	Yes	Yes	Yes	No	No	No	No
Set up Falcon Fusion SOAR workflows that view asset management data Must be paired with the Workflow Author role	Yes	Yes	Yes	Yes	No	No	No
View Falcon Fusion SOAR workflows with asset management-based triggers	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View host groups in Host Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Falcon Management

	Falcon Administrator	Exposure Management Manager	Exposure Assets Admin	Exposure Assets Analyst	Falcon Security Lead	Falcon Investigator	Falcon Analyst - Read Only
Add application hashes to custom IOCs	Yes	No	No	No	No	No	No
View custom IOCs	Yes	No	No	No	Yes	Yes	Yes

Roles for external surface attack management

Roles available in the Falcon Exposure Management or Falcon Surface subscriptions provide users with access to Falcon EASM.

Falcon Surface roles:

- External Attack Surface Admin
- External Attack Surface Read Only

Falcon Exposure Management roles:

- Falcon Admin
- Exposure Management Manager

Roles for vulnerability management (Spotlight)

These roles are included in the Falcon Exposure Management and Falcon Spotlight subscriptions.

- Vulnerability Manager:
 - View all vulnerability management dashboards, tables, and details
 - Export and manage vulnerability reports
 - Remotely patch Windows-based hosts

Note: Vulnerability Managers must also have either the RTR Active Responder or RTR Administrator role to patch hosts.

- View Falcon Fusion SOAR workflows

Note: Falcon Administrators can also create and manage Fusion SOAR workflows. Vulnerability Managers must have the Workflow Author role to create and manage workflows.

Roles for configuration assessment

- Configuration Assessment Manager:
 - Create and edit configuration assessment rules
 - Assign configuration assessment rule groups to configuration assessment policies
 - Assign configuration assessment policies to host groups
- These roles can view configuration assessment policies, rule groups, and activity:
 - Configuration Assessment Analyst
 - Falcon Security Lead
 - Falcon Investigator
 - Falcon Analyst - Read Only

Falcon Management

Roles for Falcon FileVantage

- Falcon Administrator:
 - Grant and revoke FileVantage Manager role.
 - Manage all FileVantage functionality, including policies and rule groups.
 - Assign FileVantage read scope to API clients.
 - Trigger workflows from FileVantage.
- FileVantage Manager:
 - Manage all FileVantage functionality, including policies and rule groups.
 - Trigger workflows from FileVantage.
- These roles can view file integrity policies, rule groups, and activity:
 - Falcon Administrator
 - FileVantage Manager
 - Falcon Security Lead
 - Falcon Investigator
 - Falcon Analyst
 - Falcon Analyst - Read Only

Roles for Falcon Firewall Management

- Firewall Manager: Create and edit firewall rules, assign firewall rule groups to firewall policies, and assign firewall policies to host groups.
- These roles can create firewall rule groups:
 - Falcon Administrator
 - Firewall Manager
- These roles can view firewall rules, rule groups, policies, and firewall events:
 - Falcon Administrator
 - Falcon Analyst
 - Falcon Analyst - Read Only
 - Falcon Investigator
 - Falcon Security Lead

Roles for Falcon Flight Control

Falcon Flight Control gives users access to the roles associated with their CID's purchased Falcon product subscriptions. For example, if a CID is subscribed to the Falcon Insight product, Flight Control provides users in that CID access to Falcon Insight roles. Your Flight Control parent and child CIDs can each subscribe to their own unique set of products to accommodate different service needs.

In Flight Control, when a child CID uses a product that is not also subscribed to by the parent CID, the following limitations apply:

- Parent CID users do not have access to any of the subscribed product's roles when signed in to the child CID.
- Aggregation and propagation features provided by the subscribed product are not available at the parent CID level.

In addition to subscribed product roles, Flight Control provides the following role for parent CID users:

- Flight Control Managed Analyst can access all areas of Falcon that support Flight Control CID [group access restrictions](#), but not other areas of Falcon.

Roles for Falcon for IT

- IT Analyst: View results from queries and actions.
- IT Evaluator: Run and view results from queries.
- IT Remediator: Run and view results from queries and actions.
- IT Query Manager: Run, manage, and view results from queries. View IT Automation policies.
- IT Administrator: Run, manage, and view results from queries and actions. View and manage IT Automation policies.
- Initiate Real Time Response (RTR) quick actions: Real Time Responder - Active Responder, Real Time Responder - Administrator

This table lists the default individual permissions assigned to roles that access IT automation features.

	IT Analyst	IT Evaluator	IT Remediator	IT Query Manager	IT Administrator
Cancel queries (osquery)	No	Yes	Yes	Yes	Yes

Falcon Management

	IT Analyst	IT Evaluator	IT Remediator	IT Query Manager	IT Administrator
Cancel queries (scripts)	No	Yes	Yes	Yes	Yes
Cancel remediations	No	No	Yes	No	Yes
Create queries (osquery)	No	No	No	Yes	Yes
Create queries (scripts)	No	No	No	No	Yes
Create remediations	No	No	No	No	Yes
Delete queries (osquery)	No	No	No	Yes	Yes
Delete queries (scripts)	No	No	No	Yes	Yes
Delete remediations	No	No	No	No	Yes
Edit queries (osquery)	No	No	No	Yes	Yes
Edit queries (scripts)	No	No	No	Yes	Yes
Execute remediations	No	No	Yes	No	Yes
Initiate actions	No	No	Yes	No	Yes
Osquery Schema - Read	No	Yes	Yes	Yes	Yes
Schedule queries (osquery)	No	Yes	Yes	Yes	Yes
Schedule queries (scripts)	No	Yes	Yes	Yes	Yes
Schedule remediations	No	No	Yes	No	Yes
View queries (osquery)	Yes	Yes	Yes	Yes	Yes
View queries (scripts)	Yes	Yes	Yes	Yes	Yes
View query (osquery) results	Yes	Yes	Yes	Yes	Yes
View remediations	Yes	No	Yes	No	Yes
View IT automation policies	No	No	No	Yes	Yes
Write IT automation policies	No	No	No	No	Yes

Roles for Falcon Forensics

- Falcon Administrator: View and download the Forensics app in Falcon console. Create and edit collections. Create and edit configurations.
- Forensics Configuration Manager: Create and edit configurations.
- Forensic Investigator: View and download the Forensics app in Falcon console. View collections and configurations.
- Forensics Queue Manager: Create and edit collections.

These roles can also download the Forensics app from Falcon console:

- Endpoint Manager
- Falcon Analyst
- Falcon Analyst - Read Only
- Falcon Security Lead

Roles for Falcon Foundry

- App Developer: Create new apps and manage all aspects of the app lifecycle through the Foundry App manager and Foundry CLI.

Falcon Management

- Falcon Administrator: Create new apps and manage all aspects of the app lifecycle through the Foundry App manager and Foundry CLI. Access the App catalog, install, update, and manage installed apps. Assign custom app roles to users in the Falcon console.

- Real Time Responder - Administrator and Real Time Responder - Active Responder: Execute Real Time Response app scripts.

Note: To add an RTR script to an app that's shared with Fusion SOAR workflows requires the Real Time Responder - Administrator role in addition to either the App Developer or Falcon Administrator role.

Roles for Falcon Identity Protection

- Falcon Administrator: Can perform all actions in Falcon Identity Protection.
- Identity Protection Administrator: Can perform all actions in Falcon Identity Protection.
- Falcon Security Lead: Can manage Identity Protection Insights, Incidents, Reports, and Threat Hunter.
- Falcon Investigator: Can manage Identity Protection Insights, Incidents, Reports, and Threat Hunter.
- Falcon Analyst - Read Only: Can view all information in Falcon Identity Protection.
- Endpoint Manager: Can see notifications and manage DC sensor installation and configurations..
- Identity Protection Policy Manager: Can manage Identity Protection Insights, Policy, and Reports. This role is only available for the Falcon Identity Threat Protection subscription.
- Identity Protection Domain Administrator: Can manage Identity Protection Insights, Reports, Threat Hunter, Notifications, and some actions on the Identity Protection Administration tab. This role is only available for the Falcon Identity Threat Protection subscription.

	Falcon Administrator	Identity Protection Administrator	Falcon Analyst - Read Only	Identity Protection Domain Administrator	Endpoint Manager	Falcon Security Lead
View insights graphs and entities	Yes	Yes	Yes	Yes	No	Yes
Manage custom insights	Yes	Yes	No	Yes	No	Yes
Manage custom reports	Yes	Yes	No	Yes	No	Yes
View entity profiles	Yes	Yes	Yes	Yes	No	Yes
Perform entity and insights actions (Actions menu)	Yes	Yes	No	Yes	No	Yes
View incidents list and incidents analytics	Yes	Yes	Yes	No	No	Yes
Perform incidents actions (Actions menu)	Yes	Yes	No	No	No	Yes
View incident exceptions	Yes	Yes	Yes	No	No	Yes
Perform incident exceptions actions (Actions menu)	Yes	Yes	No	No	No	Yes

Falcon Management

	Falcon Administrator	Identity Protection Administrator	Falcon Analyst - Read Only	Identity Protection Domain Administrator	Endpoint Manager	Falcon Security
View policies	Yes	Yes	Yes	No	No	Yes
Manage policies	Yes	Yes	No	No	No	No
View reports	Yes	Yes	Yes	Yes*	No	Yes
Manage reports	Yes	Yes	No	Yes*	No	Yes
View Threat Hunter events	Yes	Yes	Yes	Yes	No	Yes
Create Threat Hunter report schedules	Yes	Yes	No	Yes	No	Yes
Save Threat Hunter custom searches	Yes	Yes	No	Yes	No	Yes
View notifications	Yes	Yes	Yes	Yes	Yes	No
Mark notifications as Read	Yes	Yes	No	Yes	Yes	No
View Domains in Administration	Yes	Yes	Yes	Yes	Yes	No
Manage Domains in Administration	Yes	Yes	No	Yes	Yes	No
View Appliances in Administration	Yes	Yes	Yes	Yes	Yes	No
Manage Appliances in Administration	Yes	Yes	No	Yes	Yes	No
View Subnets in Administration	Yes	Yes	Yes	Yes	Yes	No
Manage Subnets in Administration	Yes	Yes	No	Yes	Yes	No
View email notifications in Administration	Yes	Yes	Yes	No	Yes	No
Manage email notifications in Administration	Yes	Yes	Yes	No	Yes	No

Falcon Management

	Falcon Administrator	Identity Protection Administrator	Falcon Analyst - Read Only	Identity Protection Domain Administrator	Endpoint Manager	Falcon Security
View Connectors in Administration	Yes	Yes	Yes	No	Yes	No
Manage Connectors in Administration	Yes	Yes	No	No	Yes	No
View Risk Configurations in Administration	Yes	Yes	Yes	Yes	No	Yes
Manage Risk Configurations in Administration	Yes	Yes	No	Yes	No	Yes
View Settings in Administration	Yes	Yes	Yes	No	Yes	No
Manage Settings in Administration	Yes	Yes	No	No	Yes	No

* - This role can only view the Insights and Activity tabs.

Roles for Falcon Insight for Mobile

- Falcon Administrator: Manage all mobile functionality, including enrollment, devices, mobile policies, and the Zero Trust Assessment dashboard.
- Mobile Admin: Manage all mobile functionality, including enrollment, devices, mobile policies, and the Zero Trust Assessment dashboard.

Falcon Management

Roles for Falcon Insight Next-Gen SIEM

- **Falcon Administrator:** Access all functionality in the console except certain Real Time Response (RTR) functionality.
- **Falcon Security Lead:** Manage detections, manage quarantined files, contain hosts, search for events, reset users' credentials, and view exclusions. View data about assets, accounts, and applications in asset management.
- **Falcon Investigator:** Manage detections, search for events, and view exclusions. View data about assets, accounts, and applications in asset management. View Falcon Sandbox submissions and reports. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. Manage Identity Protection insights, incidents, reports, and threat hunter. View FileVantage file integrity policies, rule groups, and activity.
- **Falcon Analyst:** Manage detections and quarantined files and view exclusions and host management. Create and manage scheduled searches and view and download the results. View Falcon Sandbox submissions and reports. View FileVantage file integrity policies, rule groups, and activity. View firewall rules, rule groups, policies, and firewall events. Download Forensics app.
- **Falcon Analyst - Read Only:** View detections and exclusions and search for events. View all Identity Protection info. View FileVantage file integrity policies, rule groups, and activity. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. View data about assets, accounts, and applications in asset management.
- **Event Viewer:** Search for events. View data about assets, accounts, and applications in asset management.
- **Endpoint Manager:** Manage sensor deployment and maintain sensor configuration and update policies. Create and edit host groups. Download Forensics app.
- **Detections Exceptions Manager:** Add, edit, and manage custom IOCs, ML exclusions, IOA exclusions, and sensor visibility exclusions.
- **Vulnerability Manager:** Manage all vulnerability management functionality.
- **Real Time Responder:** Roles are required to connect to hosts using Real Time Response. See Real Time Responder roles for more information.
- **Device Control Manager:** View device control dashboards and change device control policies.
- **Custom IOAs Manager:** Create, edit, and manage custom IOA rules, rule groups, policy assignments, and host groups.
- **MSSP Co-Managed NG-SIEM Admin:** This role is for Managed Security Service Providers (MSSPs) in customer CIDs where Falcon Complete manages first-party endpoint, identity, or cloud detections and the MSSP manages third-party detections in Next-Gen SIEM. It allows users to view detections managed by Falcon Complete while managing Next-Gen SIEM detections. This role can:
 - Access customer data needed for SIEM integration
 - Access event data streams
 - Access logs and events
 - Configure event types for streaming
 - Configure SIEM integration settings
 - Create and manage SIEM connectors
 - Create new users
 - Manage SIEM configurations for assigned customers
 - Monitor event delivery status
 - View and modify SIEM streaming settings
 - View assigned customer environments
 - View configuration settings
 - View detection data
- **NG SIEM Administrator:** Assign and revoke other Next-Gen SIEM roles, view and search Next-Gen SIEM events, manage Next-Gen SIEM detections, and perform response actions. Create and manage Next-Gen SIEM scheduled searches and custom Next-Gen SIEM detection queries. Create, view, and manage connectors, parsers, alerts, and alerts settings.
- **NG SIEM Security Lead:** View and search Next-Gen SIEM events, manage Next-Gen SIEM detections, perform response actions. Create Next-Gen SIEM scheduled searches and custom Next-Gen SIEM detection queries.
- **NG SIEM Analyst:** View and search Next-Gen SIEM events, manage Next-Gen SIEM detections, and perform response actions. Create Next-Gen SIEM scheduled searches.
- **NG SIEM Analyst - Read Only:** View and search Next-Gen SIEM events and view Next-Gen SIEM detections.
Note: Although this role is labeled as read-only, users with this role can still create Next-Gen SIEM scheduled searches.

	Falcon Administrator	Falcon Security Lead	Falcon Investigator	Falcon Analyst	Falcon Analyst - Read Only	Event Viewer	Endpoint Manager	Detections Exceptions Manager
Manage incidents and detections	Yes	Yes	Yes	Yes	No	No	No	No
Manage exclusions	Yes	No	No	No	No	No	No	Yes
Contain hosts	Yes	Yes	No	No	No	No	No	No
Search events	Yes	Yes	Yes	No	Yes	Yes	No	No

Falcon Management

	Falcon Administrator	Falcon Security Lead	Falcon Investigator	Falcon Analyst	Falcon Analyst - Read Only	Event Viewer	Endpoint Manager	Detections E
Change detection settings	Yes	No	No	No	No	No	No	No
Manage custom IOCs	Yes	No	No	No	No	No	No	Yes
View device info in asset management ¹	Yes	Yes	Yes	No	Yes	Yes	No	No
Manage sensor deployment	Yes	No	No	No	No	No	Yes	No
Reset users' credentials	Yes	Yes	No	No	No	No	No	No
Add/remove users	Yes	No	No	No	No	No	No	No
Manage API credentials	Yes	No	No	No	No	No	No	No
Connect to hosts	No	No	No	No	No	No	No	No
View Real Time Response sessions	Yes	No	No	No	No	No	No	No
View Device Control Dashboards	Yes	Yes	Yes	Yes	No	No	No	No
Change Device Control Policies	Yes	No	No	No	No	No	No	No
Create and edit custom IOAs and assign custom IOA rules to prevention policies	Yes	No	No	No	No	No	No	No
Share and edit shared customizable dashboards	Yes	No	No	No	No	No	No	No
Manage host groups	Yes	No	No	No	No	No	Yes	No
Create, view, and manage connectors, parsers, alerts, and alerts settings	Yes	No	No	No	No	No	No	No

Falcon Management

¹ - Requires a subscription with asset management access.

Roles for Falcon MalQuery

- MalQuery Admin: Use all MalQuery features, such as search, hunt, and monitor. Give other users access to MalQuery.
- MalQuery User: Use all MalQuery features, such as search, hunt, and monitor.

	MalQuery Admin	MalQuery User
Use MalQuery Search, Hunt, and Monitor	Yes	Yes
Grant the MalQuery User role to others	Yes	No

Roles for Falcon OverWatch

Users that are assigned the OverWatch Malware Submitter role can see and use the Submit Malware page ([Counter Adversary Operations > Managed Services > OverWatch malware submissions](#)). This role is automatically assigned to all users in an organization that is protected by OverWatch. Users with a Falcon Administrator role can also manage those assignments.

The following roles require one of these subscriptions:

- Falcon Adversary OverWatch Endpoint
- Falcon Adversary OverWatch Cloud
- Falcon Adversary OverWatch Cloud Containers
- Falcon Adversary OverWatch Identity

	OverWatch Endpoint Admin	OverWatch Endpoint Analyst	OverWatch Cloud Admin	OverWatch Cloud Analyst	OverWatch Identity Admin	OverWatch Identity Analyst
Access intelligence dashboards	Yes	Yes	Yes	Yes	No	No
Access basic information about adversaries and malware families	Yes	Yes	Yes	Yes	Yes	Yes
Access snapshot and hunting leads	Yes	Yes	Yes	Yes	No	No
View vulnerability intelligence	Yes	Yes	Yes	Yes	No	No
View indicator information	Yes	Yes	Yes	Yes	No	No
Submit samples to Sandbox and get reports	Yes	Yes	Yes	Yes	No	No
Create exposed credential monitoring rules and view notifications	No	No	No	No	Yes	Yes

Falcon Management

Roles for Falcon Prevent

- **Falcon Administrator:** Access all functionality in the console except certain Real Time Response (RTR) functionality.
- **Falcon Security Lead:** Manage detections, manage quarantined files, contain hosts, search for events, reset users' credentials, and view exclusions. View data about assets, accounts, and applications in asset management. Create and run on-demand scans from the Falcon console.
- **Falcon Analyst:** Manage detections and quarantined files and view exclusions and host management. Create and manage scheduled searches and view and download the results. View Falcon Sandbox submissions and reports. View FileVantage file integrity policies, rule groups, and activity. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. Create and run on-demand scans from the Falcon console.
- **Falcon Analyst - Read Only:** View detections and exclusions and search for events. View all Identity Protection info. View FileVantage file integrity policies, rule groups, and activity. View firewall rules, rule groups, policies, and firewall events. Download Forensics app. View data about assets, accounts, and applications in asset management. View on-demand scan results in the Falcon console.
- **Quarantine Manager:** View, release, and manage quarantined files.
- **Endpoint Manager:** Manage sensor deployment and maintain sensor configuration and update policies. Create and edit host groups. Download Forensics app.
- **Detections Exceptions Manager:** Add, edit, and manage custom IOCs, ML exclusions, IOA exclusions, and sensor visibility exclusions.
- **Remediation Manager:** View and manage remediation actions taken by the Falcon console.

	Falcon Administrator	Falcon Security Lead	Falcon Analyst	Falcon Analyst - Read Only	Quarantine Manager	Endpoint Manager	Detections Exceptions Manager
Manage detections	Yes	Yes	Yes	No	No	No	No
Manage exclusions	Yes	No	No	No	No	No	Yes
Manage quarantined files	Yes	Yes	Yes	No	Yes	No	No
Change prevention settings	Yes	No	No	No	No	No	No
Manage custom IOCs	Yes	No	No	No	No	No	Yes
Manage sensor deployment	Yes	No	No	No	No	Yes	No
Reset users' credentials	Yes	Yes	No	No	No	No	No
Add/remove users	Yes	No	No	No	No	No	No
Manage API credentials	Yes	No	No	No	No	No	No
Enable/Disable Detections	Yes	No	No	No	No	No	No
Share and edit shared customizable dashboards	Yes	No	No	No	No	No	No
Endpoint security > Monitor > Remediation	Yes	No	No	No	No	No	No

Falcon Management

	Falcon Administrator	Falcon Security Lead	Falcon Analyst	Falcon Analyst - Read Only	Quarantine Manager	Endpoint Manager	Detections Exceptions Man
Manage host groups	Yes	No	No	No	No	Yes	No
Manage hidden and deleted hosts	Yes	No	No	No	No	No	No

Roles for scheduled reports

- **Scheduled Report Admin:** Can assign and revoke the Scheduled Report Analyst role, create scheduled reports, view and manage any scheduled report in the CID, and view, download, and delete any generated report in the CID.
- **Falcon Administrator and Intel Admin:** Can assign and revoke the Scheduled Report Admin role plus perform any function given to All other roles.
- **Scheduled Report Analyst:** Can only access the Scheduled reports page and view and download generated reports of scheduled reports that have been specifically shared with them. You can assign this role to members of your team who need to access scheduled reports but do not need any other Falcon access. For example, you might assign this role to IT staff who need to access periodic reporting metrics to stay on top of vulnerabilities.
- **All other roles:** Can create scheduled reports, view and manage their own scheduled reports, and download and delete reports generated from their scheduled reports. They can also view and download reports generated from scheduled reports that have been shared with them.

Roles for Falcon Shield

These are the available roles for Falcon Shield.

- **Falcon Shield Owner:**
 - Control global settings.
 - Dismiss security checks in their subset of security settings.
- **Falcon Shield Admin:**
 - Control ongoing actions, including settings for alerts and reports.
 - Dismiss security checks in their subset of integrations.
- **Falcon Shield Viewer:**
 - Read-only access to the Falcon Shield console.
- **Falcon Shield Scoped Admin:**
 - Control administrative access.
 - Create and set up integrations.
 - Dismiss security checks in their subset of integrations.
- **Falcon Shield Scoped Users:**
 - Read-only access to a subset of the connected and monitored SaaS integrations.

Access Scopes

Limit user access to Next-Gen SIEM detections and advanced event search data with access scopes.

Overview

Limit user access to Next-Gen SIEM detections and advanced event search data with access scopes. Use access scopes to limit which users have access to data, based on type of detection, data connection, or vendor. Access scopes provide fine-grained access (FGA) controls on top of role-based access controls (RBAC).

Requirements

- One of the following subscriptions:
 - Falcon Insight XDR
 - Falcon Next-Gen SIEM
- Default roles:
 - Falcon Administrator
- CrowdStrike clouds:
 - US-1, US-2, EU-1, and US-GOV-1

Understanding access scopes

Use Next-Gen SIEM access scopes to limit users' access to data.

- **Event search results:** Limit access to advanced event search data, whether generated by CrowdStrike or third-party data connections.
- **Detections:** Limit access to specific types of detections, based on vendor, product, and category.

By default, users have access to all detections and event search data.

When access scopes limit a user's access to data, a notification message appears on the Advanced Event Search and User Profile pages.

Falcon Management

How multiple access scopes work together

If you have multiple access scopes assigned, they work together to expand your access to data. For example, if your access scopes grant access to both Okta and Zscaler detections, you'll see detections from both sources.

How access scopes relate to host groups and cloud groups

When you grant access to CrowdStrike first-party data with access scopes, the data is filtered further based on the user's host groups and cloud groups.

- Host groups and cloud groups apply to detections
- Cloud groups apply to advanced event search data

Granting all access scopes

When you assign access scopes to users, use the All access scopes option to grant access to all detections and advanced event search data, including for new data connections added in the future.

When you select multiple access scopes to assign to a user, you grant access to the data connections included in those access scopes. To include data from sources added in the future, you must manually update the user's access scopes.

Limitations and considerations

Important: In order for access scopes to appropriately grant access to third-party data, ensure vendor information is included when you configure your data connector.

- To access endpoint detections, a user must also have a host group assignment that gives them access to the host.
- When you configure access scope detection filters, you grant access based on the specific detection vendor, product, and category. To grant access to detections from the same vendor and product, but a different category, update the access scope accordingly.
- You can create up to 200 access scopes.
- In rare cases, advanced event search results might take longer for users with many access scopes or complex access scope filters.

Setup

Requires complete setup. In order to use access scopes to limit access to Next-Gen SIEM detections and advanced event search data, you must complete all setup steps, including creating access scopes and assigning them to users.

Managing access scopes

Create an access scope

1. Go to [Host setup and management](#) > [Falcon users](#) > [Access scope management](#).
2. Click [Create new access scope](#).
3. Enter a name and description.
4. Click [Next](#).
5. Add filters for advanced event search data.
 - a. Click [Add event filter](#).
 - b. To grant access to data generated by CrowdStrike, select [CrowdStrike first party](#).
 - c. To grant access to data generated by third-party sources, select one or more data connections. You can also use the filter options to narrow the list.
 - d. Click [Save selection](#).
6. Add filters for detections.
 - a. Click [Add detection filter](#).
 - b. Select one or more filter options.
 - c. Click [Save selection](#).
7. Click [Next](#).
8. Click [Add users](#).
 - a. Select the users to which this access scope applies. You can also use the filter options to narrow the list.
 - b. Click [Save selection](#).
9. Click [Submit](#).

Edit an access scope

1. Go to [Host setup and management](#) > [Falcon users](#) > [Access scope management](#).
2. For the access scope that you want to edit, from the Open menu , click [Edit access scope](#).
3. Modify the settings as described in [Create an access scope](#).
4. Click [Submit](#).

Delete multiple access scopes at once

1. Go to [Host setup and management](#) > [Falcon users](#) > [Access scope management](#).
2. Select multiple access scopes.
3. Click [Delete access scopes](#).
4. Click [Delete](#).

Falcon Management

Assign access scopes

You can assign access scopes to users when you create or edit an access scope. For more info, see [Create an access scope](#). You can also assign existing access scopes from [Host setup and management > Falcon users > User management](#).

Assign access scopes to a single user

1. Go to [Host setup and management > Falcon users > User management](#).
2. For the user you'd like to assign access scopes, from the Open menu , select [View details](#) page.
3. Click [Assign access scopes](#).
4. Select one or more access scopes to apply to the user. You can start typing to narrow the list.
5. Click [Assign](#).

Delete an access scope

1. Go to [Host setup and management > Falcon users > Access scope management](#).
2. For the access scope that you want to delete, from the Open menu , click [Delete access scope](#).
3. Click [Delete](#).

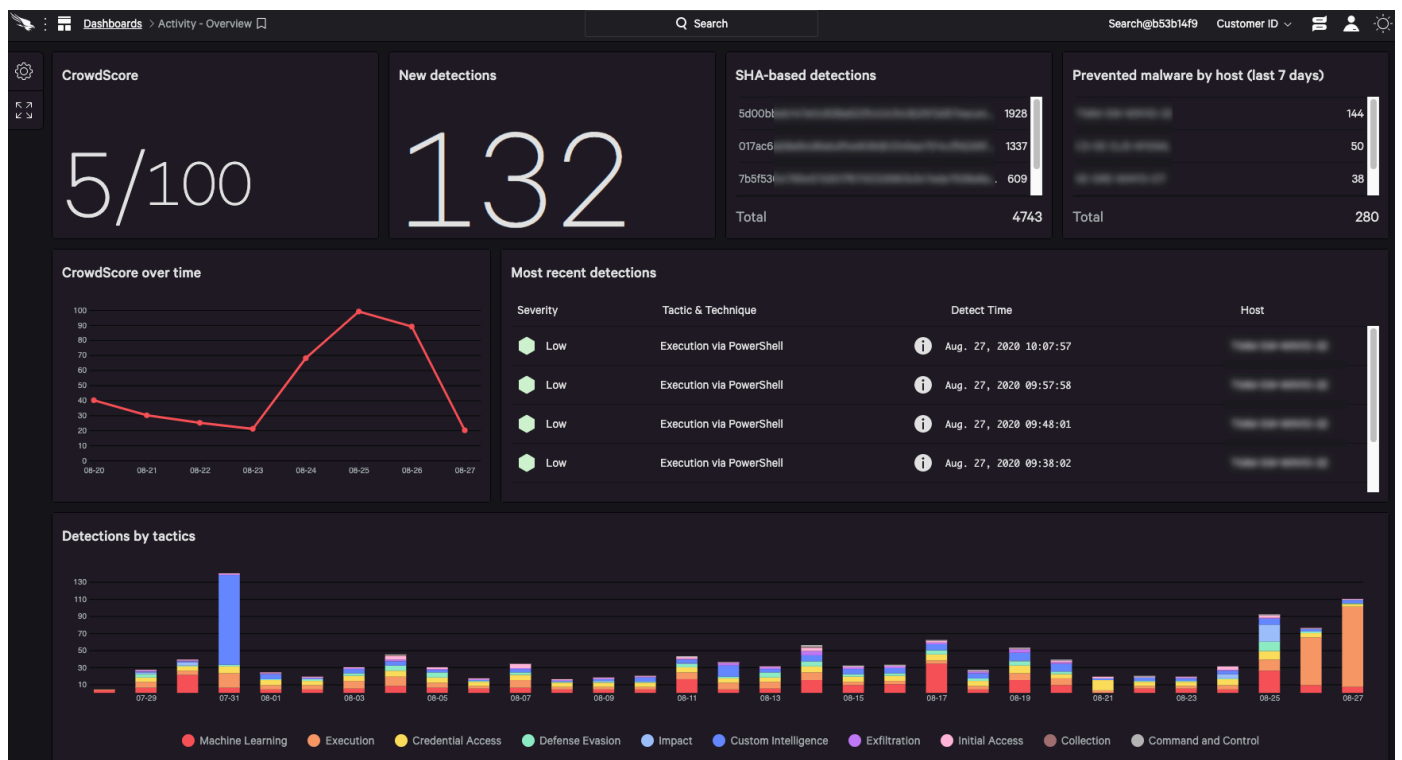
Dashboards and Reports

Customizable Dashboards

Create and manage customizable dashboards to help gain up-to-date, customized visibility into your Falcon environment.

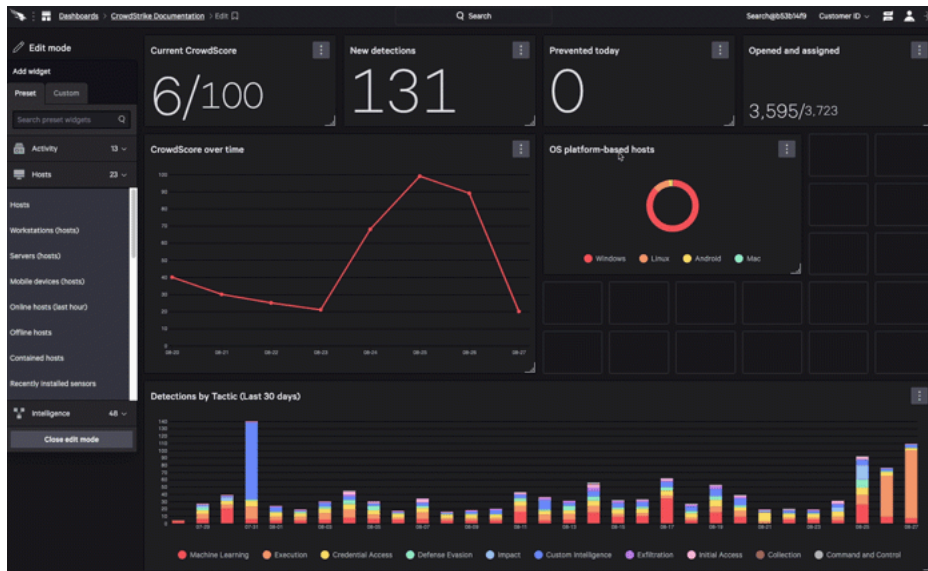
Overview

The Falcon console's customizable [Dashboards](#) provide up-to-date, customizable visibility into your Falcon environment. Dashboards show counts, graphs, and trends about your Falcon environment, including detections, current CrowdScore, host info, adversaries and Intelligence, and more.



Use the preset dashboards to see preconfigured views of commonly useful data. To surface specific details or summarize unique combinations of info for your organization's needs, you can create your own customized dashboards. When you're done, you can keep a dashboard view private, or you can share your dashboard with other users in your organization.

Falcon Management



Requirements

- Subscription: Any subscription can see basic Falcon info. Additional Falcon subscriptions, such as Falcon Intel, offer more dashboard data types.
- Roles:
 - To view all dashboards, and to create or edit private dashboards: Any Falcon role other than [Falcon Console Guest](#)
 - To share dashboards and edit shared dashboards: [Falcon Admin](#), [Intel Admin](#), or [Dashboard Admin](#) role

Note: Dashboard Admin is an add-on role. Users with this role must have at least one other role assigned to access the Falcon console.

Before you begin

To see info in Falcon's dashboards, your organization must have the relevant subscription and you must have the required user roles. The subscriptions and user roles required depend on the info shown in each dashboard.

Understanding Falcon dashboards

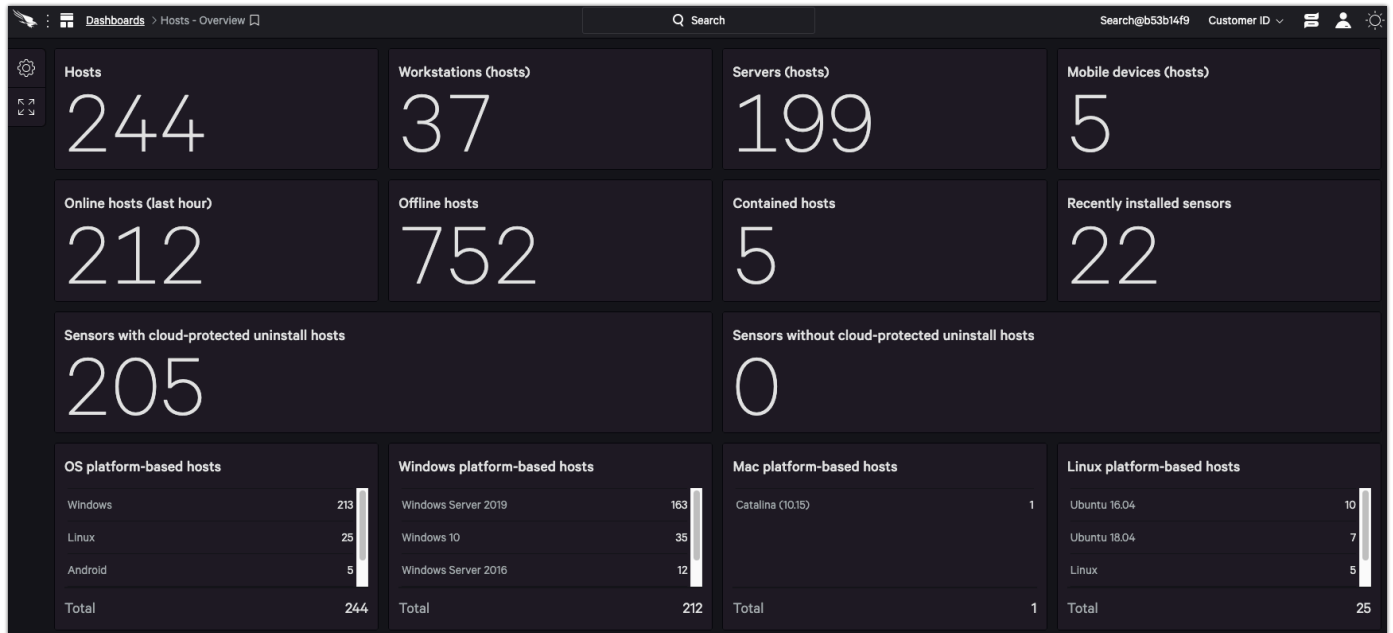
A [dashboard](#) is a particular view of info from your Falcon environment. Each dashboard is made up of one or more [widgets](#), which are graphical representations of info such as graphs, counts, or lists. Each dashboard also belongs to a [group](#). Groups indicate what type of info a dashboard shows.

The [Legacy](#) group indicates a dashboard that hasn't yet been converted to our new editable dashboard structure. Links are included here for convenience, but you can't duplicate and edit them yet.

Dashboards				Create dashboard
All Private Shared Preset				
Filter all dashboards				
Group	Name	Created by	Last modified	
Hosts	Overview	CrowdStrike	-	
Activity	Overview	CrowdStrike	-	
Intelligence	Falcon X Actors	CrowdStrike	-	
Intelligence	Falcon X Indicators	CrowdStrike	-	
Intelligence	Sandbox	CrowdStrike	-	
Intelligence	Falcon X Reports	CrowdStrike	-	
Legacy	Spotlight	CrowdStrike	-	
Legacy	Executive Summary	CrowdStrike	-	
Legacy	Detection Activity	CrowdStrike	-	

Falcon Management

For example, the preset [Hosts Overview](#) dashboard includes widgets for total hosts, host types, online hosts, hosts by platform, and more.



In your private and shared dashboards, you can add, remove, move, resize, or change the data types and filters for each widget.

Info sources for dashboards

Each widget retrieves info from a single data type, such as host info or detections. Preset dashboards usually contain info about a single area of Falcon, such as hosts, detections, or intel. However, in custom dashboards, you can combine widgets from any data types into a single dashboard. Each widget in a dashboard refreshes about once per minute.

Dashboards include info from these areas of the Falcon platform:

- Activity
- Cloud Security
- Asset management
- Falcon Complete
- FileVantage
- Hosts
- Identity Protection
- Intelligence
- Investigate
- OverWatch
- Vulnerability management
- Charlotte AI - Detection triage

Note: You can also create vulnerability management dashboards from custom filters. For more info, see [Vulnerability Monitoring](#). Watch our [feature release notes](#) for news when we add more preset dashboards and data types to our dashboards.

Dashboard types: editing and sharing

There are multiple types of Falcon dashboard:

- [Preset](#)
- [Private](#)
- [Shared](#)

Preset dashboards

Preset dashboards are built into Falcon and can't be edited. However, you can duplicate them and edit the copy. All preset dashboards are visible to all users in your organization.

Legacy dashboards

Legacy dashboards are preset dashboards that haven't yet been converted to our new editable dashboard structure. Click a legacy dashboard in this list to view the original dashboard, but you can't edit them.

Falcon Management

Private dashboards

A private dashboard is one that you've made by duplicating an existing dashboard or creating a new dashboard.

When you duplicate or create a dashboard, it's private by default. Only you can see and edit your private dashboards. Other users can't see or edit them.

Shared dashboards

You can share your private dashboards to let other users with the Dashboard Administrator role in your organization see and edit them. As with any Falcon data, users in other organizations can't see or edit them.

Single and multi source dashboards

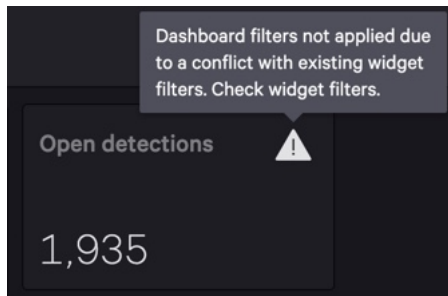
When creating a dashboard, you can choose whether the info in the dashboard comes from a single data source or multiple data sources.

Both types of dashboards can display widgets for any type of available data. However, while multi source dashboards can contain widgets for multiple data types, single source dashboards are limited to just one type. For example, a single source dashboard configured for host data can display only host widgets, and you can't add other widget types, such as detections or news, to that host dashboard. A multi source dashboard has no such restrictions and can contain widgets for hosts, detections, news, and more.

The advantage of single source dashboards is that you can apply filters across all data in the dashboard to further customize the information you see. For example, you might want a dashboard that displays critical detection activity for a certain set of hosts. You can create a single source dashboard for detections and configure filters based on severity and host name.

Because you need the same data type to apply these filters, the filter bar is not available for multi source dashboards. You must apply filters to widgets individually.

To avoid data conflicts, there are cases where a filter might not be applied to certain widgets. For example, you might have a single source dashboard for detection data. One of the widgets in the dashboard displays detections from the past 45 days. If you apply a dashboard-wide filter for detections in the past hour, the filter won't be applied to that widget.



Setup

No setup is required before using Dashboards . Dashboards are available to all Falcon users.

Managing dashboards

You can use Falcon's preset dashboards, customize an existing dashboard, or create a blank dashboard and add widgets yourself.

Getting to Dashboards

Find your dashboards in Falcon at [Dashboards](#) , including:

- Dashboards and reports > Dashboards > All dashboards: Every dashboard you can view
- Dashboards and reports > Dashboards > Private dashboards: Dashboards that you've customized or created, but not shared to your organization
- Dashboards and reports > Dashboards > Shared dashboards: Dashboards that other you or users in your organization have customized or created, then published
- Dashboards and reports > Dashboards > Preset dashboards: Dashboards that are preconfigured and can't be changed

Viewing dashboards

View dashboards in the Falcon console at [Dashboards](#) .

Dashboards

Create dashboard

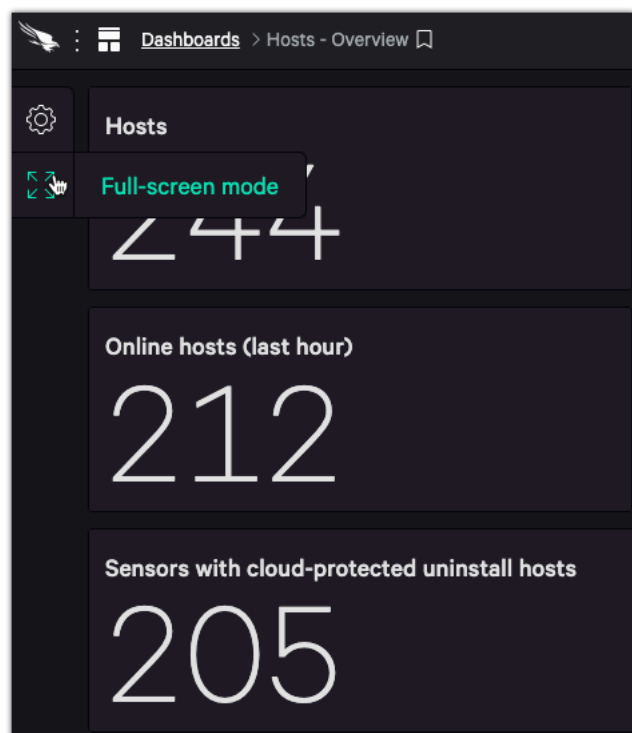
AllPrivateSharedPreset

Filter all dashboards

Group	Name	Created by	Last modified
Hosts	Overview	CrowdStrike	-
Activity	Overview	CrowdStrike	-
Intelligence	Falcon X Actors	CrowdStrike	-
Intelligence	Falcon X Indicators	CrowdStrike	-
Intelligence	Sandbox	CrowdStrike	-
Intelligence	Falcon X Reports	CrowdStrike	-
Legacy	Spotlight	CrowdStrike	-
Legacy	Executive Summary	CrowdStrike	-
Legacy	Detection Activity	CrowdStrike	-

Note: Remember to use the Falcon console's bookmarks for easy access to your most-used dashboards.

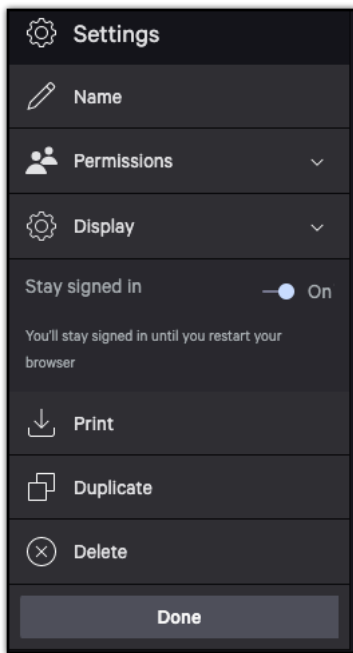
To view a dashboard at a larger size, click Full-screen mode in the left menu.



Stay signed in when viewing dashboards

To keep any dashboard permanently signed in to Falcon, enable Stay signed in in its Settings. When Stay signed in is on, Falcon does not automatically sign you out after a period of time. For example, you might use this option to keep a dashboard visible on a large display in your IT department or SOC.

1. On a dashboard, click Settings on the left side.
2. Click Display.
3. Turn on Stay signed in.



Adding a dashboard

There are two ways to add new dashboards:

- Duplicate a dashboard: Choose this to get a quick start based on an existing dashboard
- Create a dashboard: Choose this to start with a blank dashboard and add each widget yourself

Duplicating a dashboard

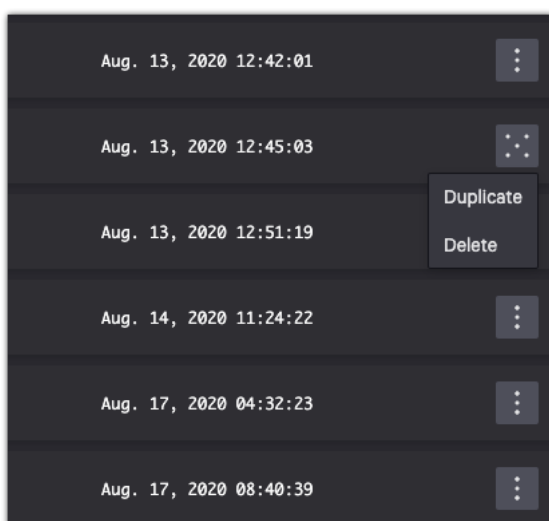
When you duplicate a dashboard, you create a second instance of that dashboard in your Falcon environment. For example, you might duplicate a preset dashboard to create an editable version of it or duplicate a private dashboard before sharing it.

Duplicated dashboards are managed independently. In other words, if you edit the original dashboard, it doesn't affect the duplicated dashboard.

If you duplicate a shared dashboard, your new dashboard is private by default. You can choose to share your new dashboard later.

To duplicate a dashboard from the main dashboards list:

1. Go to the [dashboard list](#).
2. For the dashboard you want to duplicate, click the menu on right side.

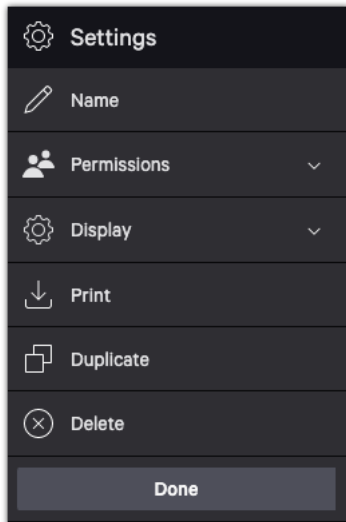


3. Click Duplicate.
4. Enter a name for the new dashboard.
5. Click Add dashboard.

To duplicate a dashboard while viewing or editing it:

1. Go to the dashboard.

2. From the  Settings menu, select  Duplicate.



3. Enter a name for the new dashboard.
4. Click Add dashboard.

After duplicating a dashboard, you can edit its widgets and share it to your organization.

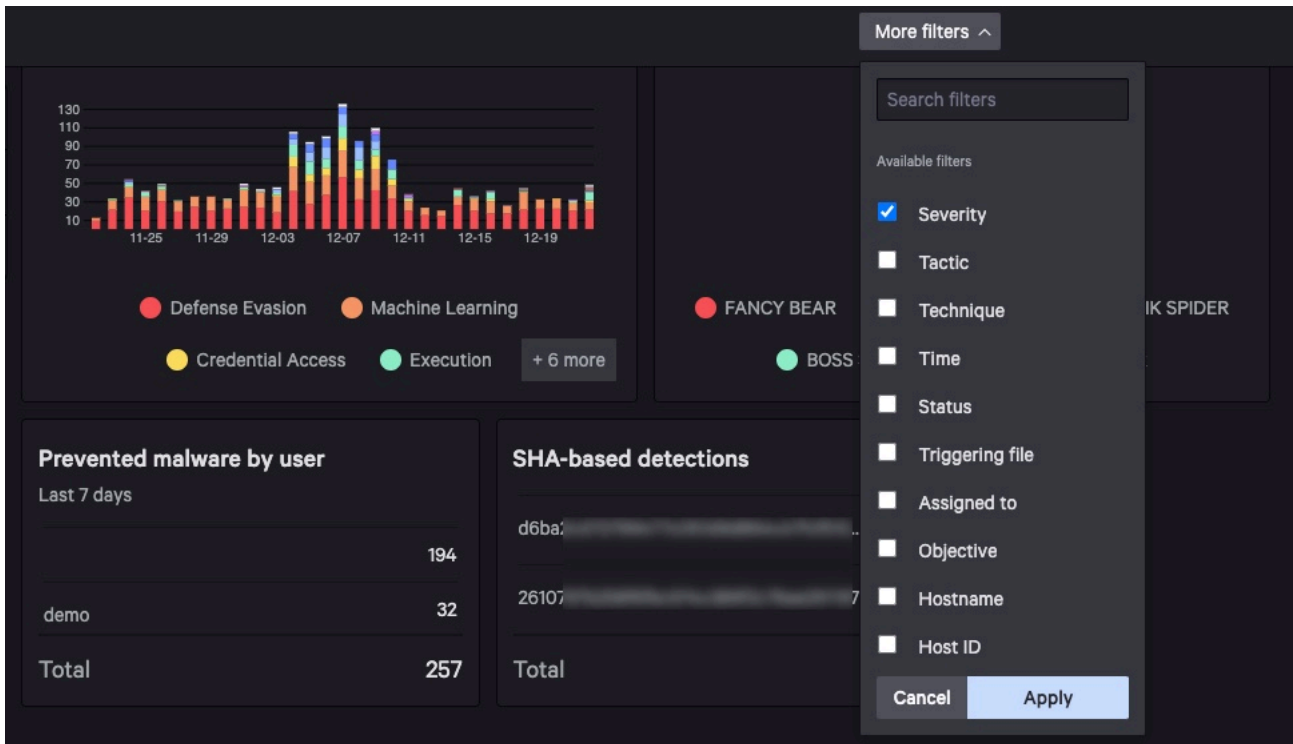
Creating a single source dashboard

Create a dashboard that contains widgets from a single data source, such as host or incident data. You can apply filters to your dashboard data to further customize the info you see.

1. Go to the [dashboard list](#).
2. Click Create dashboard.
3. Enter a name for the new dashboard.
4. Select Use data from a single source and select the data source.
5. For Activity, asset management, Intelligence, vulnerability management, or Identity Protection data sources, select the data type.
6. Click Create dashboard.

Note: After you create a dashboard, an empty grid for widgets appears.

7. Use the left menu to add widgets to your dashboard. For more info, see [Managing widgets](#).
8. Click Close edit mode.
9. If needed, apply filters to all widgets to fine-tune the displayed data.



- Click More filters.
- Select one or more filters and click Apply.
The applied filters appear next to the More filters menu.
- Click a filter.
- Select one or more items to filter and click Apply.

After creating a dashboard, you can edit its widgets and share it to your organization.

Creating a multi source dashboard

Multi source dashboards can display widgets for multiple types of data. You can't apply dashboard-wide filters to these dashboards but you can configure filters for widgets individually.

- Go to the dashboard list.
- Click Create dashboard.
- Enter a name for the new dashboard.
- Select Use data from multiple sources.
- Click Create dashboard.

Note: After you create a dashboard, an empty grid for widgets appears.

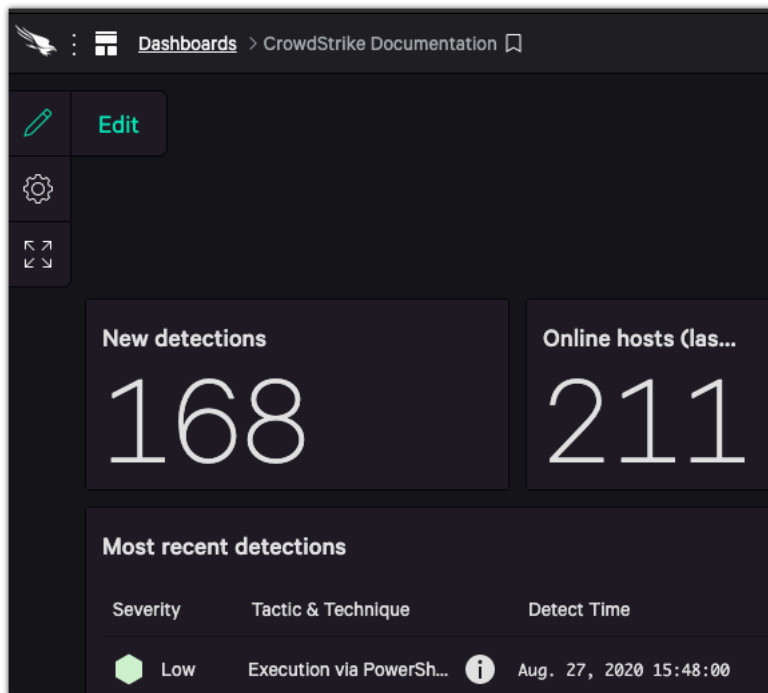
- Use the left menu to add widgets to your dashboard. For more info, see [Managing widgets](#).
- Click Close edit mode.

After creating a dashboard, you can edit its widgets and share it to your organization.

Editing a dashboard

When you edit a dashboard, you can choose new widgets, move them on the dashboard, and change data types and visualizations for each individual widget.

Only private and shared dashboards can be edited. Preset dashboards can't be changed, but you can duplicate a preset dashboard and edit the duplicate.

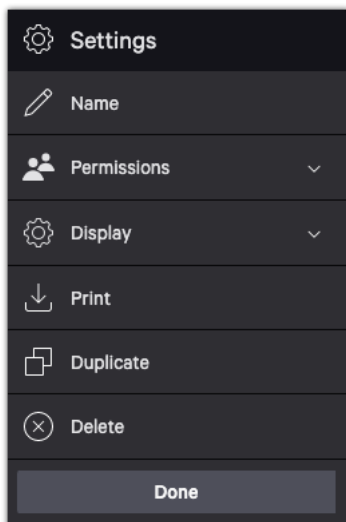


To edit a private or shared dashboard:

1. Go to the dashboard.
2. From the menu at the left side, click Edit.
3. Manage this dashboard's widgets: add widgets, edit widgets, or move them on the dashboard grid.
Note: Any changes you make are saved automatically.
4. After you're done, click Close edit mode.

To rename a dashboard:

1. Go to the dashboard.
2. From the menu at the left side, click Settings > Name.



3. Enter the new name.
4. Click Rename dashboard to save the new name.

Managing widgets

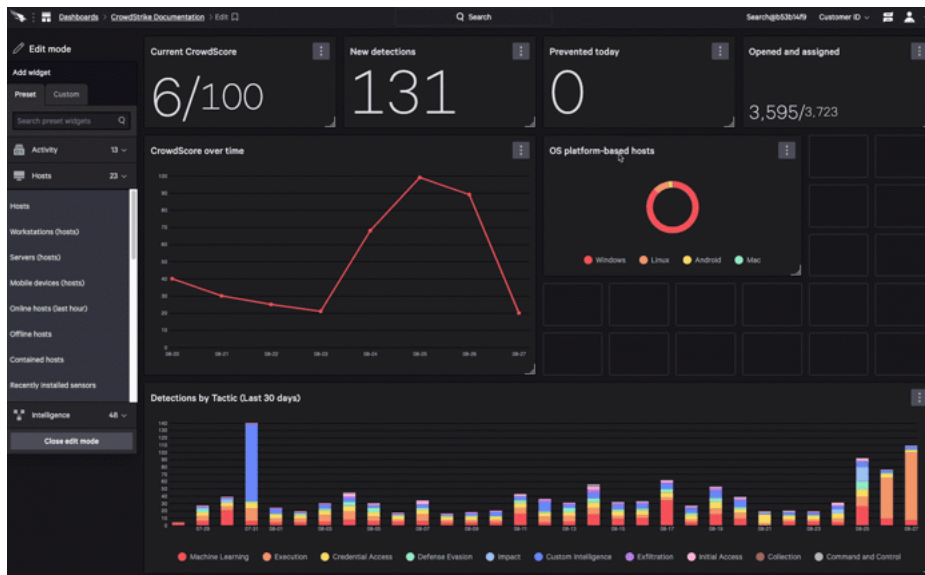
Moving and resizing a widget

When you're moving a widget, you can see the dashboard's grid. Widgets are always aligned to this grid. The grid represents the dashboard's space for widgets, which automatically scales to different screen sizes so that your widgets can be read on any screen. The grid is always 12 units wide, but it can be any height. The grid automatically adds new units at the bottom when you add or move widgets there.

Falcon Management

To reorganize widgets on a dashboard:

1. Go to a private or shared dashboard.
2. Click Edit.
3. Interact with individual widgets:
 - Move widgets by clicking and dragging them.
 - Resize widgets by clicking and dragging the arrow indicator in the bottom-right corner of each widget.



Note: When you use a dashboard in full-screen mode, you can't scroll down to see more widgets. If you plan to use full-screen mode for a given dashboard, organize your widgets so that all the widgets fit to the height of your display.

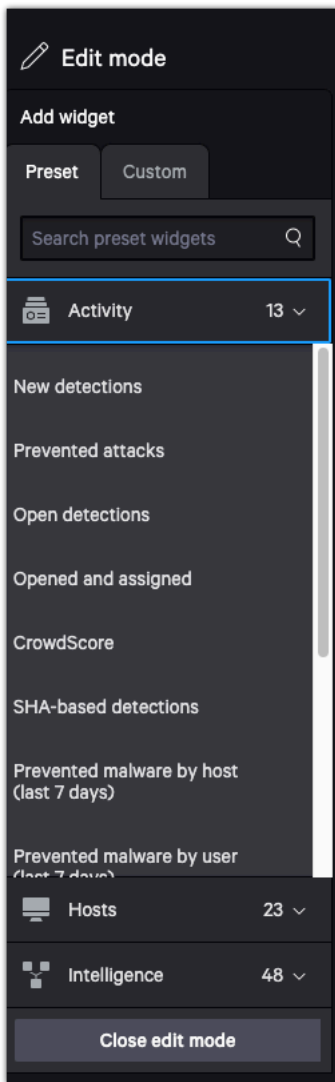
Adding a preset widget

Falcon's dashboards include many preset widgets. These widgets are used to build the preset dashboards. They're configured with sensible defaults, so you can use them in your own dashboards without having to do extra configuration.

To add a preset widget:

1. Go to a private or shared dashboard.
2. Click Edit.
3. From the menu on the left, click a data type, such as Activity or Hosts, to view the preset options for that type of Falcon data.

Note: If you're modifying a single source dashboard, you'll see only one type of widget.
4. Click a widget's name to add that widget to your dashboard.



After adding a preset widget, you can optionally edit its settings to adjust the info you see.

Creating or editing a custom widget

Fine tune the info in your widgets by editing an existing widget or even creating a new one. You can edit any widget on a private or shared dashboard, but not widgets on a preset dashboard.

In most cases, we recommend editing an existing widget rather than creating a new widget. It's usually quicker and easier to change a widget that's close to your needs than to build a new custom widget. However, creating a widget can be the best way to tailor it to your organization's needs.



To create or edit a widget:

1. Go to a private or shared dashboard.
2. Click Edit.
3. Select a widget:
 - o Edit an existing widget: click the menu in the widget's upper-right corner.
 - o Create a new widget: click Custom in the menu on the left.
4. In the menu on the left, choose settings for this widget. After you make enough selections, the widget preview shows you what the widget will look like.

Note: You might not be able to modify some settings for certain widgets. For example, you can't modify the data type for widgets in a single source dashboard.

- a. Widget data: Choose an area of Falcon to display data from, such as Activity or Hosts. Many data types have subtypes. For example, Activity has Detections, Quarantined files, and more.
- b. Widget data filters: Limit the widget's data to specific attributes and sub-attributes, including time filters.
- c. Widget appearance: Configure how the widget is displayed.
 - i. Widget title: Optionally provide a label that replaces the default widget title. If you don't enter a title, the widget will use the data type as a default label.
 - ii. Display widget as: Choose how your data type is displayed, such as a line chart or donut chart.
 - iii. Display data by: Choose how to divide the data in your widget. For example, in a donut chart for detections, you might divide your chart into segments by severity, the host's platform, or the host's domain.

Note: Some chart types, such as Count, don't support dividing data.

5. Click Add widget or Save widget to save your widget and return to the dashboard.

Using time filters in dashboard widgets

Time can be reflected in many different ways in your dashboard data. When configuring line charts and stacked bar charts, some widget data types let you apply multiple time-based filters to fine-tune how your data is presented.

For example, if you have a dashboard displaying detection data, you can apply filters based on when the detection was found and when the affected host was first seen. This dashboard has four widgets, each displaying detection data in different ways based on the combination of configured time filters:



1. Detections in the last 30 days, displayed by week

This widget shows all detections in the last 30 days, grouped by the week the detection was found.

2. Detections in the past 30 days, displayed by when the host was first seen

Although the data in this widget is the same as widget #1 — it contains the same number and type of detections — the X axis goes beyond 30 days. In this example, a detection appears for the week of October 7th of a previous year. Although the detection occurred in the past 30 days, the host it was found on was first seen by Falcon in that week of October.

3. Detection Time and Host First Seen of last 30 days, displayed by detection time found

This widget shows detections that were found in the past 30 days and found on hosts that were first seen on Falcon in the past 30 days, displayed by the week the detection was found.

This configuration is helpful to get a sense of detection activity on your newer hosts.

4. Detection Time and Host First Seen of last 30 days, displayed by host first seen

This widget shows the same data as widget #3 but the detections are displayed by when the host was first seen and not when the detection was found.

To configure widget #1 — show detections found in the past 30 days, displayed by week — use these settings:

- Widget data
 - Falcon data category: Activity
 - Falcon data type: Detections
- Widget data filters
 - More filters: Time
 - Time: Last 30 days
- Widget appearance
 - Display widget as: Stacked bar chart
 - Display time by: Time
 - At intervals of: Week
 - Display data by: Actor

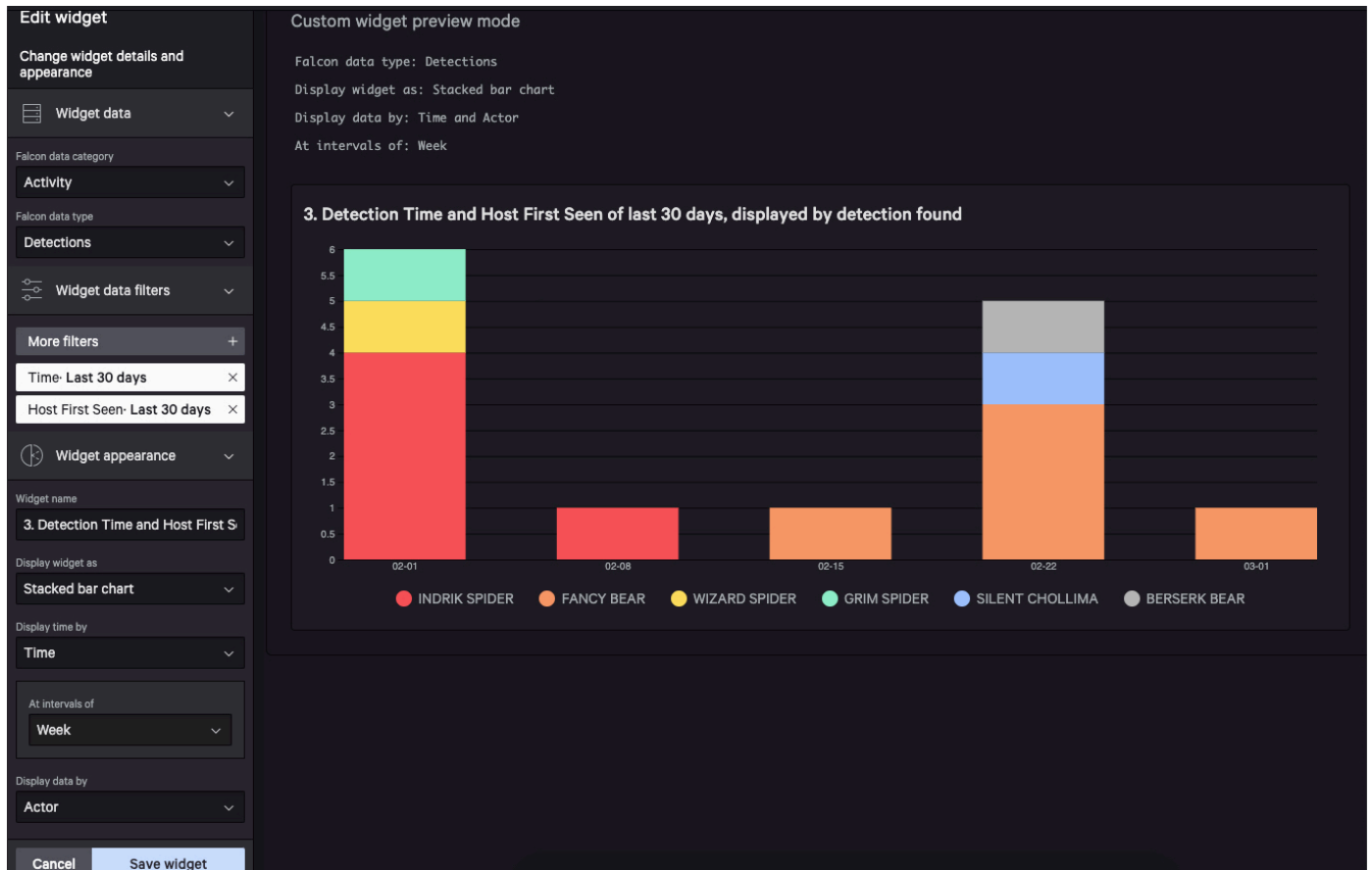




To configure widget #3 — show detections found in the past 30 days and found on hosts first seen on Falcon in the past 30 days, displayed by detection time — use these settings:

- Widget data
 - Falcon data category: Activity
 - Falcon data type: Detections
- Widget data filters
 - More filters
 - Time
 - Host First Seen
 - Time: Last 30 days
 - Host First Seen: Last 30 days
- Widget appearance
 - Display widget as: Stacked bar chart
 - Display time by: Time
 - At intervals of: Week
 - Display data by: Actor

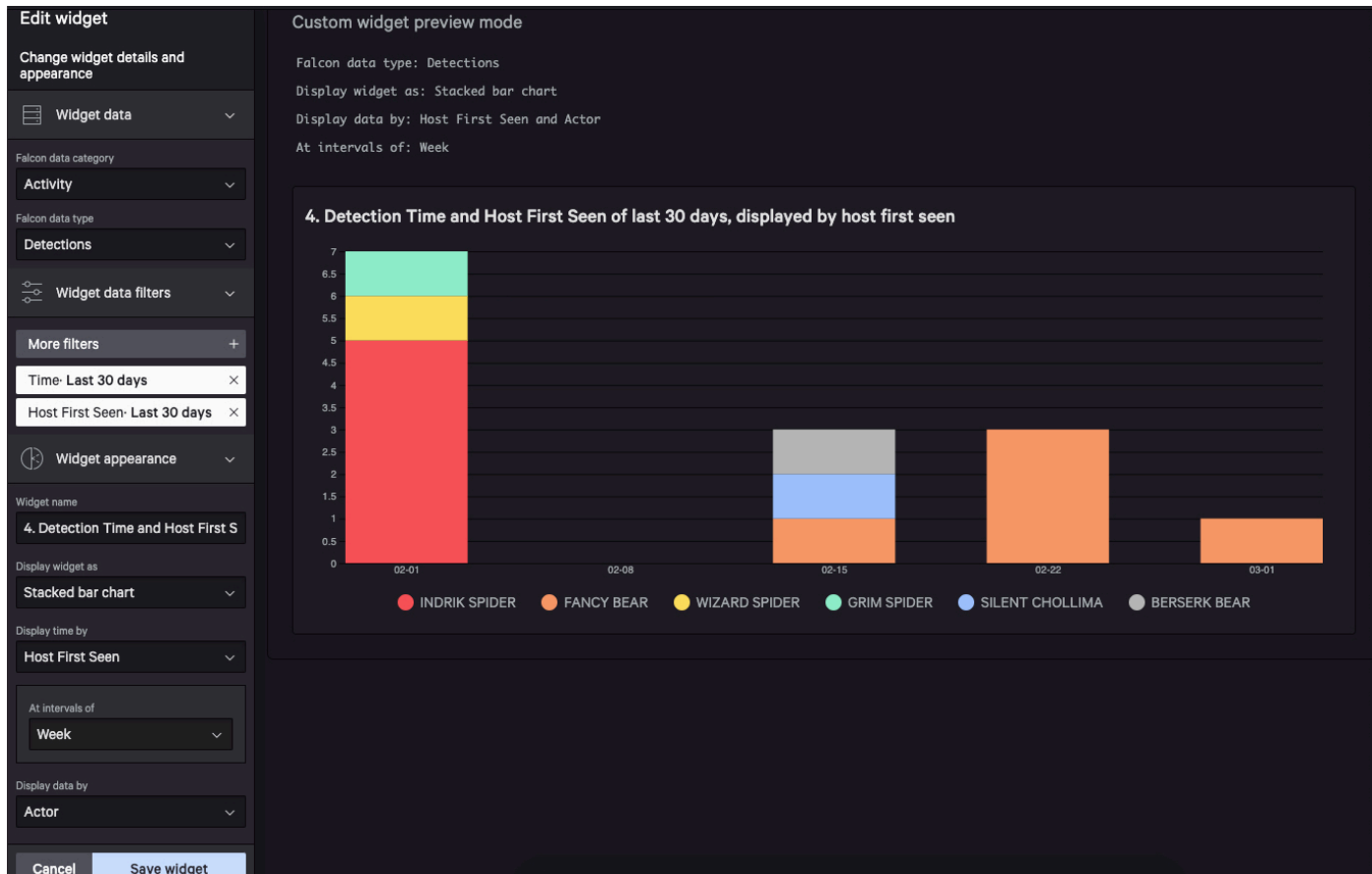
Falcon Management



To configure widget #4 — show detections that were found in the past 30 days and found on hosts that were first seen on Falcon in the past 30 days, displayed by host first seen — use these settings:

- Widget data
 - Falcon data category: Activity
 - Falcon data type: Detections
- Widget data filters
 - More filters
 - Time
 - Host First Seen
 - Time: Last 30 days
 - Host First Seen: Last 30 days
- Widget appearance
 - Display widget as: Stacked bar chart
 - Display time by: Host First Seen
 - At intervals of: Week
 - Display data by: Actor

Falcon Management



Sharing a dashboard

By default, your custom dashboards are private. You can choose to share them to your organization, but after a dashboard is shared, you can't make it private again.

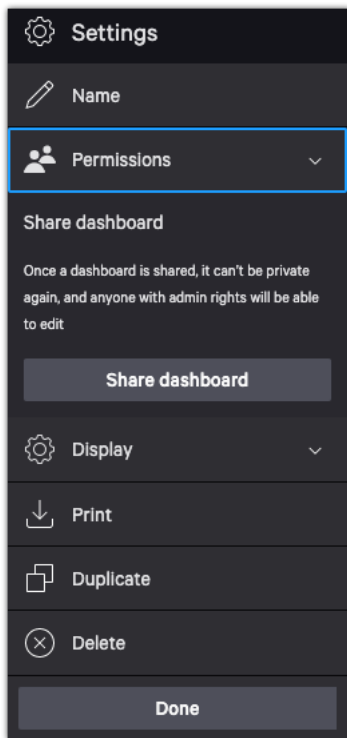
- Private: Only you can see and edit your private dashboards. Other users can't see or edit them.
- Shared: Other admin users in your organization can see, edit, and delete your shared dashboards. Users outside your organization can't see or edit them, as with all your Falcon info.

You must have a user role of Falcon Admin, Intel Admin, or Dashboard Admin role to share dashboards.

Note: Before sharing a dashboard, consider duplicating it to keep a private backup copy. For example, admin users can delete shared dashboards, so you might want to keep a private copy.

To share a private dashboard:

1. Go to the dashboard
2. From the menu at the left side, click Settings > Permissions



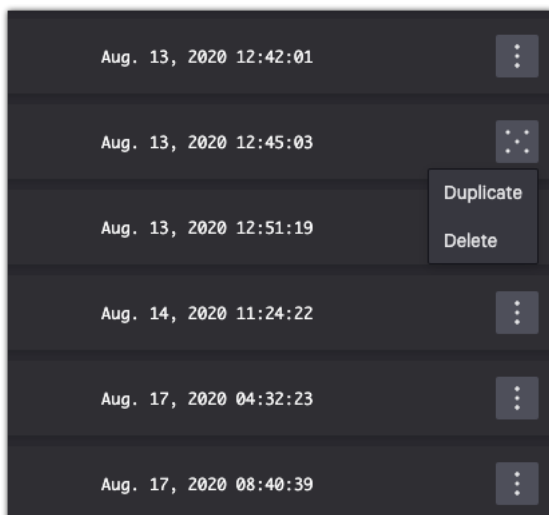
3. Click Share dashboard
4. When asked, click Share dashboard to confirm

Deleting a dashboard

Deleting a dashboard permanently removes it from Falcon. If a dashboard is shared with your organization, it's deleted for all users. Deleted dashboards can't be recovered.

To delete a dashboard from the main dashboards list:

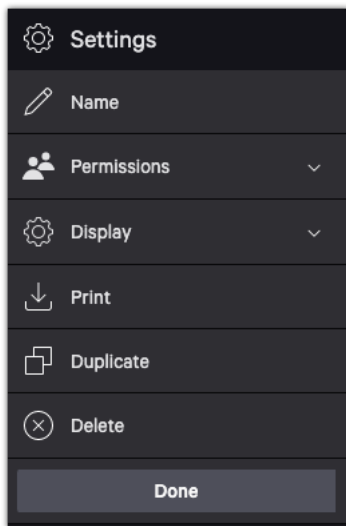
1. Go to the [dashboard list](#).
2. For the dashboard you want to delete, click the menu on right side.



3. Click Delete.
4. When asked, click Delete dashboard to confirm.

To delete a dashboard while viewing or editing it:

1. Go to the dashboard.
2. From the menu at the left side, click Settings > Delete.



3. When asked, click Delete dashboard to confirm.

Scheduled Reports

Create scheduled reports to get automatic, recurring updates of the data that matters most to you.

Overview

Create scheduled reports to get automatic, recurring updates of the data that matters most to you. You can download and share your scheduled reports, and receive a notification each time a new report is available.

For example, you might schedule reports for:

- A weekly summary of hosts in your environment
- Daily counts of hosts with critical vulnerabilities
- A monthly snapshot of the Executive Summary dashboard

Requirements

Default roles

- Scheduled Report Admin: Can assign and revoke the Scheduled Report Analyst role, create scheduled reports, view and manage any scheduled report in the CID, and view, download, and delete any generated report in the CID.
- Falcon Administrator and Intel Admin: Can assign and revoke the Scheduled Report Admin role plus perform any function given to All other roles.
- Scheduled Report Analyst: Can only access the Scheduled reports page and view and download generated reports of scheduled reports that have been specifically shared with them. You can assign this role to members of your team who need to access scheduled reports but do not need any other Falcon access. For example, you might assign this role to IT staff who need to access periodic reporting metrics to stay on top of vulnerabilities.
- All other roles: Can create scheduled reports, view and manage their own scheduled reports, and download and delete reports generated from their scheduled reports. They can also view and download reports generated from scheduled reports that have been shared with them.

CrowdStrike clouds

- Scheduled reports are supported across all CrowdStrike clouds.
- Slack, PagerDuty, Microsoft Teams, and webhook notifications are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.
- Email attachments are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.

Understanding scheduled reporting

Scheduled reports eliminate the need for manual report generation by providing automated, continuous updates of important metrics that you can share with your team. You specify the data to include, when the report runs, and who to notify when a new report is available. You can create scheduled reports with customized sets of host, vulnerability management, asset applications, or cloud security data. You can also schedule reports that provide a regular snapshot of various dashboards. Scheduled reports can run daily, weekly, or monthly at a time you choose, and you can notify designated recipients when new reports are available through email, Slack, PagerDuty, Microsoft Teams, or webhook. After creating a scheduled report, you can view and manage the report settings, manually run reports on demand, and download generated report files from the Scheduled reports page.

Falcon Management

Scheduled report settings

When creating a new scheduled report, you customize settings in four main sections.

- **Report data:** The underlying data that populates the report
- **Report details:** Basic report information, such as name, description, and output format
- **Report schedule:** When to run the report and how often
- **Notifications:** Delivery destinations for new report notifications

Report data

A new scheduled report begins with a Falcon data source that specifies the type of data you want to see in the report. Depending on the data source you select, additional filtering options may be available to narrow the scope of the data that displays.

Data source

You can build a scheduled report from any of the following data sources you have access to:

Data source type	Description
Dashboard	Schedule automated generation of your Private, Shared, and Preset dashboards at Dashboards and reports > Dashboards > All dashboards .
Hosts	Schedule reports with data from the Host Management page at Host setup and management > Manage endpoints > Host management .
FileVantage	Schedule reports with data from the File Integrity Changes page at FileVantage > File integrity monitoring > Changes .
Assets - Applications	Schedule reports with data about applications that are installed or used in your environment at Exposure management > Applications > Applications .
External assets	Schedule reports with data from the External assets page at Exposure management > Assets > External assets . For info about migrating legacy UI alerts to Falcon-native UI scheduled reports, see Mapping legacy UI alerts to Falcon-native UI scheduled reports .
Vulnerability management > Installed patches	Schedule reports with data from Installed Patches at Exposure management > Vulnerability management > Installed patches .
Vulnerability management > Vulnerabilities	Schedule reports with vulnerability data from the Vulnerabilities page at Exposure management > Vulnerability management > Vulnerabilities. For more info, see Create scheduled vulnerability reports Tip: You can base scheduled reports on saved export templates. Reports can include: • Vulnerability data • Vulnerability data and evaluation test results • Remediation data
Vulnerability management > Remediations per asset (Legacy)	Schedule reports with remediation data from the Vulnerabilities page at Exposure management > Vulnerability management > Vulnerabilities .
Vulnerability management > Vulnerabilities with evidence	Schedule reports with vulnerability evaluation test results from the Vulnerabilities page at Exposure management > Vulnerability management > Vulnerabilities .
Cloud security > IOM posture	Schedule reports with indicators of misconfiguration (IOM) findings in your cloud environment at Cloud security > Cloud posture > Indicators of misconfiguration (IOMs) .
Cloud security > IOA posture	Schedule reports with indicators of attack (IOA) findings in your cloud environment at Cloud security > Cloud posture > Cloud indicators of attack (IOAs) .
Cloud security > Image vulnerabilities	Schedule reports with information on packages and vulnerabilities found in your container images. This information is also available on the Image vulnerabilities and Packages tabs at Cloud security > Vulnerabilities > Image assessments .
Cloud security > Container vulnerabilities	Schedule reports with information on all packages and vulnerabilities found in running containers that match the criteria you specify. This information is also available on the Containers tab at Cloud security > Assets > Kubernetes and containers inventory .
Cloud security > Container details	Schedule reports with details about containers that match the criteria you specify. This information is also available on the Containers tab at Cloud security > Assets > Kubernetes and containers inventory .

Falcon Management

Data source type	Description
Cloud security > Image detections	Schedule reports with information on detections such as malware, secrets, and CIS benchmark deviations found in your container images. This information is also available on the Detections tab at Cloud security > Vulnerabilities > Image assessments .
Cloud security > Containers and images compliance	Schedule reports with information on CIS benchmark deviations found in your container images. This information is also available on the Detections tab at Cloud security > Compliance > Containers and images .
Cloud security > Function vulnerabilities	Schedule reports with data about serverless function vulnerabilities discovered in your cloud environment. For more info, see Monitor Serverless Functions .
Cloud security > Function detections	Schedule reports with data about preruntime detections discovered in your cloud environment. For more info, see Monitor Serverless Functions .
Configuration assessment	Schedule reports with data about configuration assessments in your environment at Exposure management > Configuration assessment > Assessments. Select one of these reports: • Summary • Group by rules • Group by rule groups • Group by assets • Summary with evidence
XIoT vulnerabilities	Schedule reports with ICS vulnerability data from Falcon Discover for IoT. For more info, see Detect Control System Vulnerabilities

Filters

Cloud security, FileVantage, configuration assessment, vulnerability management, host, and XIoT vulnerability data sources provide additional filters that you can use to customize the report data that displays. Filter options vary by data source. If no filters are applied, your report contains all available data from the selected source.

For FileVantage sources, select the data you want to add to the report. Add or remove data columns either manually or with a template to determine what appears in your scheduled report. Apply optional filters to the data.

Dashboard types

The Dashboard data source requires you to select a specific dashboard to report on. Dashboard reports include all data from the selected dashboard and do not allow additional filtering.

Usage notes:

- You can only schedule reports for dashboards you have access to.
- The scheduled reporting feature does not support Legacy dashboards.

Data details

The asset applications data source requires additional data to determine the report data that displays. Select application groups or one or more individual applications and vendors, and then apply criteria. For info about application groups, see [Create application groups](#).

You can select applications that are installed or not installed, or are used or not used.

Apply the filters you want to the data, such as the host groups to include in the report. Note that hidden assets aren't included in scheduled report data. If you don't apply filters, your report contains all available data from the selected source.

Report details

In the Report details section, provide basic information that defines your report.

Falcon Management

- **Name:** Provide a descriptive name for the scheduled report. The name identifies the report on the Scheduled reports page. It also appears in report notifications.
- **Description:** Enter an optional description to briefly define the report contents or purpose.
- **File format:** Choose a file format for generating your reports.
 - Vulnerability management and host reports: JSON (default) or CSV
 - Dashboard reports: PDF
 - Cloud Security reports: JSON or CSV (default)
 - FileVantage reports: JSON or CSV (default)
 - Asset applications reports: JSON or CSV (default)
 - External assets reports: JSON or CSV (default)
- **Shared with:** Specify the users to share your report with. Users on this list are your account users that are entered in Falcon. You can share the report with up to 10 users. Your scheduled report will appear on shared users' Scheduled reports page with options to view the report history and download generated reports.

Report schedule

Scheduled reports generate automatically according to the schedule you set. Choose the time, day, and interval to run your report. You also choose the reporting period duration by selecting the first day the report should be generated and an optional end date. You can configure the schedule to run your report daily, weekly, monthly, twice a day, or on multiple days in a week or month.

When setting up the report schedule, configure the following options:

Start date

The date to begin running the scheduled report. In the Falcon console, you can select the next day or any date in the future. From the Scheduled reports and searches APIs, you can select the current date as a start date. Falcon will generate a new report at the next scheduled interval following the designated Start date. It's not possible to backdate the start of a report.

End date

The date to stop running the report. This is an optional field that you can use to schedule your report to run for a specific period of time only. For example, if you want to run your report for a four-month period, you can set an End date that occurs four months after the Start date.

Keep these considerations in mind when specifying an End date:

- After the End date is reached, no new reports are made for this scheduled report.
- The End date must be on or after the report's Start date.
- The End date cannot be modified after a scheduled report is saved.
- If an End date is not specified, the report runs indefinitely, beginning on the Start date.

Frequency

The recurring interval at which the report will run. The frequency can be set to Daily, Weekly, or Monthly.

- **Daily report:** Generate reports on a daily basis at a designated time. You can schedule a report to run up to two times a day. For example, you can schedule a report to run every Friday at 8AM and 5PM.
- **Weekly report:** Generate reports weekly. You can select one or more days and up to two times to run the report each day. For example, you can schedule a report to run every Monday, Wednesday, and Saturday at midnight and 11AM.
- **Monthly report:** Generate a report monthly. You can select one or more days of the month and up to two times to run the report on those days. For example, you can schedule a report to run at 6AM on the 1st and 15th of each month. **Note:** The monthly day selection is limited to days of the month that appear in every month (1st–28th). Reports needed from the 29th–31st of the month can be run [on demand](#).

Time

The hour of day to run the report from 12AM (midnight) to 11PM UTC time. All scheduled reports use UTC time regardless of the time zone of the report. For example, if you are in Pacific Standard Time (PST) and schedule a report to run on Tuesdays at 7AM UTC, the report will run on Mondays at 11PM PST. If you want your report to run at 7AM PST, choose 3PM UTC in the scheduler.

You can use the US time zone calculations below as a guide to help ensure you're scheduling the right UTC time for running your reports. Decide what time you want to run the report in your local timezone and then add the appropriate number of hours to get the corresponding UTC time. For example, to run a report at 6AM EDT, select 10AM UTC.

Falcon Management

- Atlantic Daylight Time: add 3 hours
- Atlantic Standard Time: add 4 hours
- Eastern Daylight Time: add 4 hours
- Eastern Standard Time: add 5 hours
- Central Daylight Time: add 5 hours
- Central Standard Time: add 6 hours
- Mountain Daylight Time: add 6 hours
- Mountain Standard Time: add 7 hours
- Pacific Daylight Time: add 7 hours
- Pacific Standard Time: add 8 hours
- Alaska Daylight Time: add 8 hours
- Alaska Standard Time: add 9 hours
- Hawaii-Aleutian Standard Time: add 10 hours
- Samoa Standard Time: add 11 hours

Notifications

Set up automatic delivery of notifications to alert members of your team each time a report is generated. You can email notifications to individual recipients or send them to groups of people through Slack, PagerDuty, Microsoft Teams, or webhook integrations. A notification contains a summary of the report metadata and a link to download the report in Falcon. In email notifications, you can also choose to send the report file as an attachment.

[External] The Weekly host report report has been generated



falcon@crowdstrike.com <falcon@crowdstrike.com>

To: Diana Hudson

Today at 11:50 AM



CROWDSTRIKE

The **Weekly host report** has been generated

Report name: Weekly host report

Data source: Hosts

Schedule: Weekly on Wednesday at 4 PM UTC

Status: Complete

You must be logged in to the Falcon console to download the report.

[Download report](#)

Copyright © 2021 CrowdStrike, Inc. All rights reserved.

Usage notes:

- To access a generated report through the notification link, a person must be a registered user in your CID and signed in to Falcon. In addition, the scheduled report must be shared with the user through the report settings (if they are not the report creator or a Scheduled Report Admin).
- The report schedule specifies the time that a report begins processing and does not indicate the notification delivery time. Notifications are sent after report processing is complete. For example, if a report takes 10 minutes to process, notifications are delivered at least 10 minutes after the report's scheduled run time.

Note: Large reports take longer to process.

- Recipients cannot unsubscribe from report notifications. The scheduled report creator or a Scheduled Report Admin must remove them from the scheduled report notification settings.

Notification delivery options

Send new generated report notifications to individual users by email or to groups of users through Slack, PagerDuty, Microsoft Teams, or webhook. You can configure one or more delivery methods for each scheduled report to ensure notifications are sent using the best method of communication for your teams.

Falcon Management

Usage notes:

- App integration through the [CrowdStrike Store](#) is required to receive Slack, PagerDuty, Microsoft Teams, or webhook notifications.
- Slack, PagerDuty, Microsoft Teams, and webhook notifications are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.
- Email attachments are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.

Email

Send scheduled report notifications to a specified list of email addresses in your approved domains. You can designate up to 10 email notification recipients per scheduled report, including people who are not Falcon users.

Email attachments

When configuring an email notification, you can choose to include generated report files as attachments (US-1, US-2, and EU-1 cloud-based accounts only). All email attachments are Base64 encoded for safe transmission. In addition, attachments containing CSV and JSON data are compressed into a ZIP file prior to Base64 encoding.

The maximum individual file size for an email attachment is 25 MB (after Base64 encoding). Note that because Base64 encoding enlarges a file by approximately 33%, there is a difference in size between files directly downloaded from Falcon and those sent as email attachments. You should consider this enlargement factor when configuring your report data and frequency to keep email attachments below the required size limit. Files that exceed 25 MB aren't included as attachments; however, the email notification includes a link to access the report in Falcon.

- Attaching reports sends data out of Falcon to systems that might have different security standards or terms and conditions.
- The file size limit for email attachments is subject to change in accordance with CrowdStrike policies.

Calculating email attachment file size

You can use the size of a report you've downloaded from Falcon to help determine whether the file meets the allowed 25 MB limit for email attachments. To account for compression and Base64 encoding in attachments, your downloaded file size should not exceed the following:

- PDF report files: 16.5 MB max download size
- CSV and JSON report files: 100 MB max download size

If a file is too large, you can adjust the report filters or run the report more frequently to reduce the size.

Slack

Route notifications to one or more channels in your integrated Slack account. A Slack integration [through the CrowdStrike Store](#) is required. For information about setting up a Slack integration, see [CrowdStrike Store App Integrations](#).

PagerDuty

Configure notifications to automatically open an incident in PagerDuty and alert relevant user groups. Select the PagerDuty source and severity from your connected service to configure notification delivery. A PagerDuty integration [through the CrowdStrike Store](#) is required. You can get more info about setting up your PagerDuty integration in [CrowdStrike Store App Integrations](#).

Microsoft Teams

Send notifications to one or more channels in your integrated Microsoft Teams account. A Microsoft Teams integration through the CrowdStrike Store is required. For info about setting up a Microsoft Teams integration, see [CrowdStrike Store App Integrations](#).

Webhook

Distribute notifications to other applications through a webhook. A webhook integration through the CrowdStrike Store is required. For info about setting up a webhook integration, see [CrowdStrike Store App Integrations](#).

Scheduled report limits

As you create your scheduled reports, be aware of the following limitations.

Falcon Management

- Your CID can have up to 25 active scheduled reports per data source.
- Scheduled Report Admins can create any number of scheduled reports, up to the CID limits.
- All roles other than Scheduled Report Admin can have up to 5 active scheduled reports per data source type. If this limit is reached, you can disable or delete an existing report that's no longer needed to make room for a new one.
- Scheduled reports allow a maximum number of results per report. Reports that exceed this limit are not generated and show an Error status on the Scheduled reports page. If your scheduled report exceeds this limit, you can try increasing the reporting frequency or applying filters to narrow the result set.
 - Reports with host or vulnerability management data: Up to 1 million entries (such as one million hosts, vulnerabilities, or rows in a CSV file) per report
 - Reports with cloud security IOM or IOA posture data: Up to 100,000 results per report
 - Reports with cloud security image vulnerability data: Up to 1 million results or 10,000 images per report, whichever is reached first.
 - Reports with cloud security container vulnerability data: Up to 1 million results or 10,000 containers per report, whichever is reached first.
 - Reports with cloud security container details: Up to 10,000 containers per report.
 - Reports with cloud security image detection data: Up to 10,000 detections per report.
 - Reports with cloud security containers and images compliance:
 - Container and images compliance summary is always limited to the data presented in the dashboard widgets.
 - Compliance by clusters: Up to 1000 clusters per report.
 - Compliance by rules: Up to 100 rules per report.
 - Compliance by images: Up to 10000 images per report.
 - Reports with FileVantage data: Up to 5 million results per report.
 - Reports with asset applications data: Up to 1 million hosts per report.
- Generated reports are retained for 30 days. After that, they are no longer available.

Manage scheduled reports

Access your scheduled reports

The Scheduled reports page at [Dashboards and reports > Dashboards > Scheduled reporting](#) lists all of the scheduled reports you can access, including reports created by you and those that have been shared with you. From this page, you can create and manage your own scheduled reports, search for reports by name, run reports on demand, and view and download generated reports.

Note for Falcon Flight Control subscribers: For details about managing scheduled reports across your parent and child CIDs, see [Falcon Flight Control and Multi-CID Support](#).

View the list of scheduled reports

View and manage your scheduled reports from the Scheduled reports page at [Dashboards and reports > Dashboards > Scheduled reporting](#) . For each scheduled report in the list, you can preview key report information at a glance and access a menu of relevant actions that can be performed.

Falcon Management

- Report name: The user-defined report name.
- Created by: The email address of the user who created the report.
- Data source: The report data source, such as Data from Hosts or Data from Dashboard.
- Data details: Shows any applied filters or, for dashboard reports, displays a dashboard name and type.
Note: The Data details field is empty in Cloud Security Posture, asset applications, host, and vulnerability management reports when no filters have been added.
- Notifications: Shows Configured or Not configured to indicate whether report notifications have been set up.
- Status: The current report status. Either Active, Updating, or Inactive.
- Last report: The timestamp of the last generated report. Scheduled reports show UTC time. The local system time displays for reports run on demand.
- Last report status: The status of the last generated report. Either Processing, Completed, Error, No report data (new report data was not available), or empty if a report has never been generated.
- Next report: The next scheduled generation date.
- For roles other than Scheduled Report Analyst, click Actions  to access these options:
 - Download current report: Download the most recently generated report
 - View report history: Open a list of the last 30 days of generated reports
 - Run report: Run the report on demand
 - Edit report details: Modify the name, description, and shared user list
 - Edit data: Update the report filters or selected dashboard
 - Edit schedule: Change the frequency, days, and times
 - Edit notifications: Add, remove, or change notification settings
 - Deactivate: Stop future scheduled report generation
 - Delete: Delete the scheduled report
- For Scheduled Report Analyst roles and shared reports, click Actions  to access these options:
 - Current report: Download the most recently generated report
 - Report history: Open a list of the last 30 days of generated reports

 [Dashboards](#) > [Scheduled reports](#)

ABC Company    

Scheduled reports 3

Create scheduled report

Filter scheduled reports 

Report name	Created by	Data source	Data details	Notifications	Schedule status	Last report	Last report status	Next report	
Weekly host report	diana.hudson@email.com	Data from Hosts		Configured	Active	Jun. 3, 2021 11:49:23	Processing	Jun. 9, 2021 09:00:00	
Monthly Executive Summary report	brad.bowen@email.com	Data from Dashboard	Executive Summary - Preset	Configured	Active	Never generated		Jun. 15, 2021 07:00:00	
Daily critical vulnerabilities report	roytien@email.com	Data from Spotlight	cve.severity:'CRITICAL'+status:'clo...	Not configured	Active	Jun. 3, 2021 11:00:00	Completed	Jun. 4, 2021 11:00:00	

[View the report history](#)

View a 30-day history of generated reports (both successful and unsuccessful) for any scheduled report. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) , then click Open menu  next to the report name you want and select View report history. The report history lists all reports generated in the last 30 days in chronological order by date, with the newest report at the top. Each report in the list includes high-level summary details and additional actions that can be performed.

Falcon Management

- **Generated:** The UTC date and time the report was generated.
- **Status:** The generated report status. Options include Processing, Completed, Error, No report data.
- **Expires:** The date and time when the system will automatically delete the report.
- **Three-dot button:** Additional actions that can be performed on the generated report. Options include Download and Delete. Delete displays only if you are the report creator or a Scheduled Report Admin.



Dashboards > Scheduled reports > Daily critical vulnerabilities report

Q Search

ABC Company  

Daily critical vulnerabilities report history

Generated	Status	Expires	
Jun. 3, 2021 11:00:00	Completed	Jul. 3, 2021 11:00:31	
Jun. 2, 2021 11:00:00	Completed	Jul. 2, 2021 11:00:33	
Jun. 1, 2021 11:00:00	Completed	Jul. 1, 2021 11:00:33	
May. 31, 2021 11:00:00	Completed	Jun. 30, 2021 11:00:34	
May. 30, 2021 11:00:00	Completed	Jun. 29, 2021 11:00:34	
May. 29, 2021 11:00:01	Completed	Jun. 28, 2021 11:00:34	
May. 28, 2021 11:00:01	Completed	Jun. 27, 2021 11:00:33	
May. 27, 2021 14:20:25	Completed	Jun. 26, 2021 14:20:56	

Create a scheduled report

Scheduled reports are created in four steps and can be configured in minutes from the Scheduled reports page at Dashboards and reports > Dashboards > Scheduled reporting . To create a report, you define the report data, details, schedule, and optional notifications. Falcon automatically generates a report with the specified data and notifies designated recipients, as scheduled.

About the report scheduler

The report scheduler is a guided workflow that walks you through each step of scheduling a report. It lets you visually track your progress and view your report content as you go. At any point during configuration, click the edit icon in a completed section on the Scheduled report summary panel to go back and modify the details. You can also click Back at the bottom of the page to return to the previous section.

Dashboards

Scheduled reports

Schedule a report

Search

ABC Company

How often should the report generate?

Choose the start date, frequency, and time of day

Start date

Jun. 4, 2021

End date (optional)

Select

Frequency

Daily

At this time

1 PM UTC

1 AM UTC

Select time

Scheduled report summary

Report data

Data source
Spotlight vulnerabilities

Data details
2 filters applied

Report details

Report name
Daily critical vulnerabilities report

Description
A daily count of host with critical vulnerabilities.

File format
CSV

Shared with
Falcon_Analyst_ent-vult@crowdstrike.com, Analyst_All_ent-vult@crowdstrike.com

Report schedule

Dates
From Fri Jun 04 2021

Frequency
Daily at 1 PM UTC, 1 AM UTC

Notifications

Not yet selected

Back

Next

Schedule a new report

Follows these steps to schedule a new report:

1. On the Scheduled reports page at [Dashboards and reports > Dashboards > Scheduled reporting](#), click **Create scheduled report**.

2. Select a **data source** for your report and click Next.

Note: A scheduled report can have only one data source.

3. Configure additional settings for your selected data source.

- o For vulnerability management and host data sources use [optional filters](#) to limit the data that displays in the report. A default set of filters displays for the data source you selected. You can use these filters to include or exclude report data in the following ways:
 - Click a dark gray filter category, select the data points you want to see in the report, and click Apply.
 - A number that displays on the right of a filter option indicates its current count. This number can change as filters are added or removed from the report.
 - With some filter options, you can click Exclude to omit a specific data point from the report.
 - As you add and remove filters, the list of valid filters you can use in your report automatically adjusts. Some filters are no longer available when other filters are selected. When this happens, a filter shows, “No results found.”
 - Your applied filters display in light gray in the filter list. Click X on an applied filter to remove it. You can also see a count of your current filters under the Data details on the Scheduled report summary panel.
- o Asset applications data source: Select applications and browser extensions in a group or individually, specify criteria, and add optional filters to limit the data that displays in the report.
 - The list of application groups comes from groups you create. For more info, see [Create application groups](#).
 - Apply criteria to your selections. You can select applications that are installed or not installed, or are used or not used.
 - Use the optional filters to include or exclude report data in the ways listed for vulnerability management and host data sources above. If this report applies to only certain assets in your environment, filter on those assets here. For more info, see [Planning and preparation](#).
- o FileVantage data source: Select the data to include, the order the data columns are displayed, and optional filters to limit the data that displays in the report.
- o Dashboard data source: Choose a [dashboard](#) to schedule for reporting. Select a value from the Dashboard type list, choose a name from the Dashboard name list, and then click Next.
- o External assets data source: Select the data to include, the order the data columns are displayed, and optional filters to limit the data that displays in the report.

Falcon Management

4. Add the following report details and then click Next.

- Enter a name for your report and provide an optional description.
- If your report contains host, FileVantage, asset applications, or vulnerability management data, choose the report format (JSON or CSV).
- Optional. In the Shared with field, select the email addresses of account users you would like to make the report available to. You can only share the report with user email addresses registered to your CID. Email addresses cannot be manually entered for report sharing.

5. Set the schedule for how often to generate the report and then click Next.

- **Start date:** Choose the first day to run the report. The current date is selected by default.
- **End date:** Provide an optional end date to schedule your report to run for a specific period of time. If no end date is provided, your report will run indefinitely.
- **Frequency:** Choose the interval at which to run the report (Daily, Weekly, or Monthly). For weekly and monthly frequencies, select one or more days of the week or month to run the report.
- **At this time:** Select the hour of the day to run the report. A report can run up to two times each day. Note that the times shown are UTC. See the report Time section for more information about working with UTC time.

6. Configure notification settings as needed. For more info, see [Scheduled report notification configuration fields](#). Skip this step to opt out of sending notifications for this scheduled report.

7. Click Save to schedule your report.

Edit a scheduled report

You can edit the settings of a scheduled report from the Scheduled reports page at [Dashboards and reports > Dashboards > Scheduled reporting](#) if you are the report creator or if you have the Scheduled Report Admin role. You cannot modify scheduled reports created by other users. You can choose to edit certain parts of the report, including the schedule, content, and notifications. The changes you make are applied in subsequent generated reports.

1. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) .

2. Next to the report with the report scheduler you want to edit, click Open menu  and select the report section you want to edit to open the report scheduler. While editing in the scheduler, you can use the edit icons on the Scheduled report summary panel to open and make changes in other report sections. These options are available to edit from the report scheduler:

- Edit report details: Modify the name, description, and shared user list.
- Edit data: Update the report filters or selected dashboard. The data source cannot be changed.
- Edit schedule: Change the frequency, days, and times. The report Start date and End date (if provided) cannot be changed. If an End date was not previously added, you can select one during the editing process.
- Edit notifications: Update notification settings, including adding or removing delivery methods and recipients.

3. Click Update report when all changes have been made.

Run a scheduled report on demand

In addition to the scheduled generation of reports, use the Run report option to generate a current report on demand. Just like reports that run on a schedule, notifications are sent to recipients and the report is saved in the report history when processing is complete.

Usage Notes*:*

- Reports that you run on demand include a timestamp based on your local system time and not UTC time.
- The Last report status does not update in real time and might show as Processing even after processing is complete. You can periodically refresh the page to get the current status, or check for the completed report in the report history. If you receive report notifications, you'll be alerted when the report is ready.

To run a report on demand:

1. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) .

2. Click Open menu  next to the report you want to run and select Run report. The report begins processing and notifies designated recipients when the Last report status shows Completed.

Download a generated scheduled report

Download generated reports to review the report content. You can download reports from the report history of scheduled reports created by you and those that other users have shared with you. Reports are downloaded in the file format specified in the scheduled report settings.

1. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) .

2. Click Open menu  next to the scheduled report in the list and select View report history.

3. Find the report you want to download. Click Open menu  and select Download.

Deactivate a scheduled report

To stop running a report, deactivate it. When a report is deactivated, its Schedule status changes to Inactive and all further report generation stops. A deactivated report cannot be reactivated. Deactivated reports are automatically deleted after 30 days.

Falcon Management

1. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) .
2. Next to the report you want to deactivate, click Open menu  and select Deactivate.

Take ownership of a scheduled report

Admin users can use the Take Ownership option to replace the owner of a scheduled report and become its owner. This is useful for reports that were created by a user who was later deleted. You must have an admin role, such as Scheduled Reports Admin, Falcon Admin, or Intel Admin, to use Take Ownership.

1. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) .
2. Click Open menu  next to the report whose owner you want to replace and select Take Ownership.

Delete a scheduled report

If you no longer need a scheduled report, you can delete it. Deleting a scheduled report permanently removes it from Falcon.

1. Go to [Dashboards and reports > Dashboards > Scheduled reporting](#) .
2. Next to the report you want to delete, click Open menu  and select Delete.

Scheduled report notification configuration fields

When configuring a scheduled report, set up notifications if you want to alert others each time that the scheduled report runs. For more info about notifications and app integrations, see [Notifications](#).

For info about configuring scheduled reports, see [Creating a scheduled report](#) or [Editing a scheduled report](#).

For each scheduled report, you can configure one or more notification methods. To set up multiple delivery methods, click [Add another notification](#) after adding a notification method.

Notification method	Description and options
Send email	Send an email notification to specific recipients each time the scheduled report runs. In the Recipients field, choose from email addresses of registered users in your CID or manually enter any email address in your approved domains and press Enter. You can enter up to 10 email addresses. To send new report notifications with the results directly attached, select the Attach report checkbox (US-1, US-2, and EU-1 cloud-based accounts only). Note that attaching results sends data out of Falcon to systems that might have different security standards or terms and conditions.
Send Slack message	Send a notification to specified Slack channels each time the scheduled report runs. Select one or more Channel options from the list.
Create a PagerDuty incident	Create a PagerDuty incident each time the scheduled report runs. Select a PagerDuty source and PagerDuty severity.
Send Microsoft Teams message	Send a notification to the specified Microsoft Teams channel each time the scheduled report runs. Select the applicable Channel name from the list.
Send webhook notification	Send a webhook notification each time the scheduled report runs. Select the applicable webhook Name from the list.

Billing and Usage

Billing Dashboards for Usage and Licensing

Learn about dashboards that provide info to monitor sensor usage compared with purchased licenses across your environment.

Billing Dashboards for Usage and Licensing

Billing dashboards deliver quick, focused access to the information you need to monitor sensor usage and purchased licenses across your environment. With this info, you can gain insight about how your licensing compares to your actual usage.

The two dashboards represent the two billing, or licensing, models that we offer.

Falcon Management

- Sensor subscription licenses dashboard: View your 4-week (28-day) average against your licenses and see the breakdown of that usage by types of endpoints.
- Reserved and on-demand licenses dashboard: View your hourly usage and compare it to your reserved licenses. Also view the percentage of your remaining on-demand prepayment and see a breakdown of the usage by types of endpoints.

Both dashboards provide views into licensing and usage.

With these dashboards, you can view this data:

- For multi-CID environments, aggregated usage data that allows you to manage your licenses more easily across your account.
- Current usage and usage trends over time that allow you to easily compare your actual usage to your licensing.
- The 4-week average for your sensor subscription licenses that also allows you to easily compare your licensing to your actual usage.
- The reserved license data and percentage of remaining on-demand prepayment that shows you when your usage exceeded the reserved license count and how that affected your prepayment balance.

Your license combination determines what you, as a Falcon Administrator, can see.

If you're in an active proof of value (POV) trial, you can compare and anticipate usage trends and manage your licensing for your environment with POV data in your billing dashboards. To enable POV view for your dashboards, see [View POV usage and licensing data](#).

Requirements

- Product bundles (at least one):

To see these dashboards, you must have at least one of the following bundles:

- Endpoint Protection Platform (EPP)
- Cloud Workload Protection (CWP)
 - Cloud Workload Protection for Public Cloud
 - Cloud Workload Protection for Cloud Service Provider Managed Containers
- Falcon Cloud Security (FSC)
- Falcon Cloud Security with Containers (FCSC)
- Falcon Managed Containers (FMC)
- CrowdStrike clouds: Available in all clouds; US-GOV-1 and US-GOV-2 CIDs require specific licenses for these bundles.
- Roles: Falcon Administrator

Licensing

For info about licensing, including how sensor usage is calculated and what makes a sensor unique, see [CrowdStrike Sensor Licensing](#).

Differences between single-CID and multi-CID environments

To see a licensing dashboard, view the dashboard using a single CID account or using a parent CID in a multi-CID account. For multi-CID accounts, the usage is aggregated across all CIDs in that account.

The dashboards support multi-CID environments where you manage the parent CIDs using Falcon Flight Control. For parent CIDs, the dashboards show aggregated usage data for the CIDs in the account compared to the purchased licenses. For a CID that's not a parent, the dashboards show usage data, but no license data, for only that CID. However, you might have multiple accounts depending on how your organization was structured with CrowdStrike. For more info, contact your account team.

View licensing with the Sensor subscription licenses dashboard

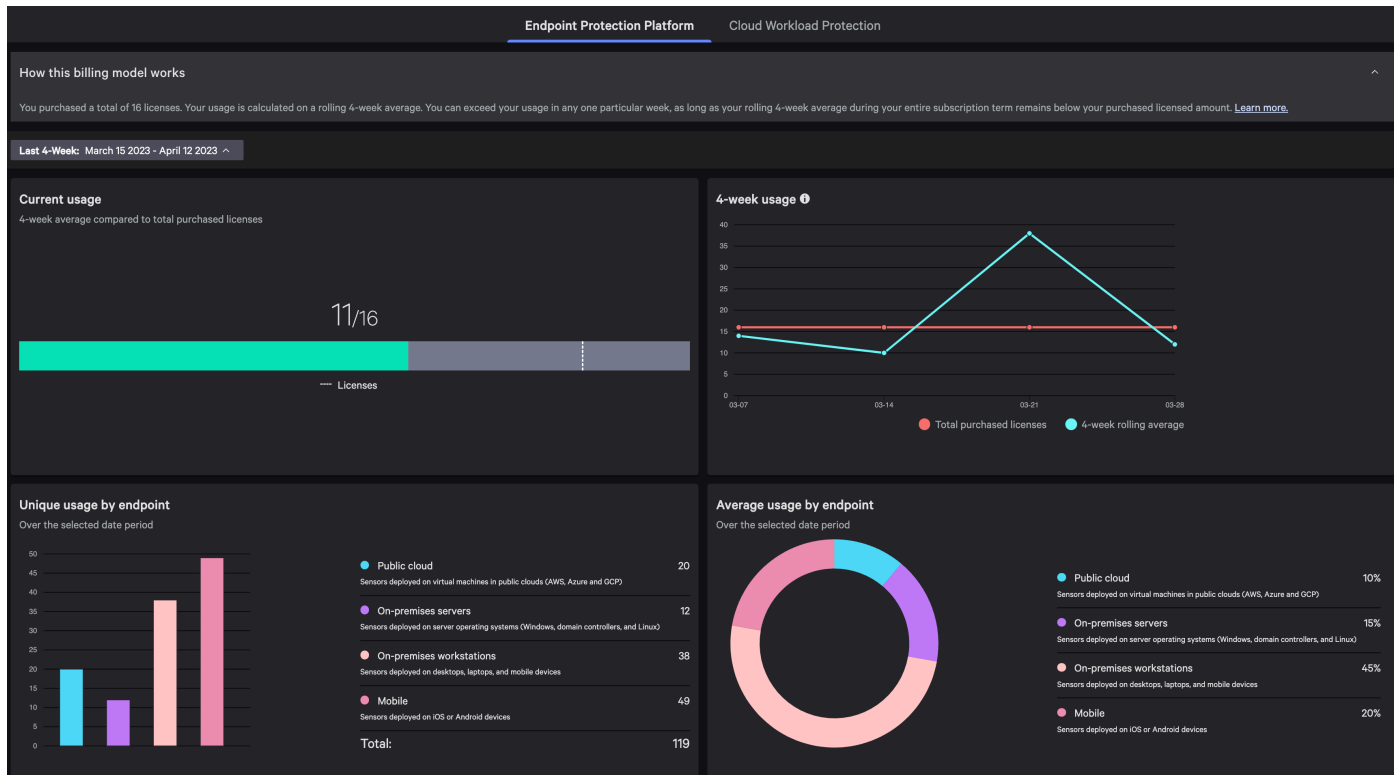
The Sensor subscription licenses dashboard provides usage data for the 4-week period you select. This period aligns with CrowdStrike's billing processes, which calculate a weekly average over the previous 4 weeks. This period is also referred to as a 4-week rolling average.

With the appropriate licensing and the Falcon Administrator role, you can access this dashboard by going to [Dashboards and reports > Billing > Sensor subscription licenses](#).

On the dashboard, select a time period to display the data for.

Note: Usage information is refreshed daily.

Falcon Management



This table explains the sections of the page.

Section	Description and usage
How this billing model works	Collapsible section that describes how this particular billing model works and provides a link to more info.
Current usage	The latest 4-week average relative to the total number of licenses purchased for the CID. The numbers are shown as a ratio over a bar chart. The 4-week average is calculated by taking the count of unique, active sensors in each of the previous 4 weeks, adding the 4 counts together, and dividing by 4.
4-week usage	Over the last 4 weeks, the 4-week rolling average and the total number of licenses purchased for the CID. The graph shows values for both items once per week for 4 weeks.
Unique usage by endpoint	Unique sensor deployments seen over the entire 4-week period, by category.
Average usage by endpoint	The percentages for the sensor deployments seen over the entire 4-week period, by category.

View licensing with the Reserved and on-demand licenses dashboard

Use the Reserved and on-demand licenses dashboard to visualize and track endpoints and workloads that are licensed hourly, see utilization by provider, and view different breakdowns of your overall sensor usage. An active sensor records a number of usage hours (1-24) per day. On-demand reporting displays hourly usage for a specified period of time. By default, usage for the current month displays.

With the appropriate licensing and the Falcon Administrator role, you can access this dashboard by going to **Dashboards and reports > Billing > Reserved and on-demand licenses**.

On the dashboard, select a time period to display the data for.

Note: Usage information is hourly but is only updated once a day.

Falcon Management



This table explains the sections of the page.

Section	Description and usage
How this billing model works	Collapsible section that describes how this particular billing model works and provides a link to more info.
Percentage of remaining on-demand prepayment	The amount of your on-demand prepayment balance that remained at the end of the previous calendar month. Note: This value doesn't reflect any usage for the current month.
Usage percentage by endpoint and workload type	The relative usage of sensors by usage category.
User percentage by public cloud	The relative usage of sensors in the public cloud by cloud provider.
Usage by license type	A breakdown of usage by license type.
Hourly sensor usage	A breakdown of hourly usage by cloud sensor provider over the specified time period. Each bar shows the total number of sensors running for all providers in a given hour with usage of reserved and unreserved resources reflected in size and color.
Reserved license	The number of reserved sensor licenses for the specified time period.
Sensor hours over reserved license	The number of hours in the time period that exceeded the reserved license count. Any usage over your reserved license count in any clock hour reduces your on-demand prepayment balance.
Hourly sensor minimum usage	The fewest number of sensors running in an hour for the specified time period.
Hourly sensor maximum usage	The greatest number of sensors running in an hour for the specified time period.

Falcon Management

View usage with the Sensor subscription licenses tab

With the appropriate licensing and the Falcon Administrator role, you can access this dashboard by going to [Dashboards and reports > Billing > Annual usage](#) and then clicking Sensor Subscription License at the top of the window.



This table explains the sections of the page.

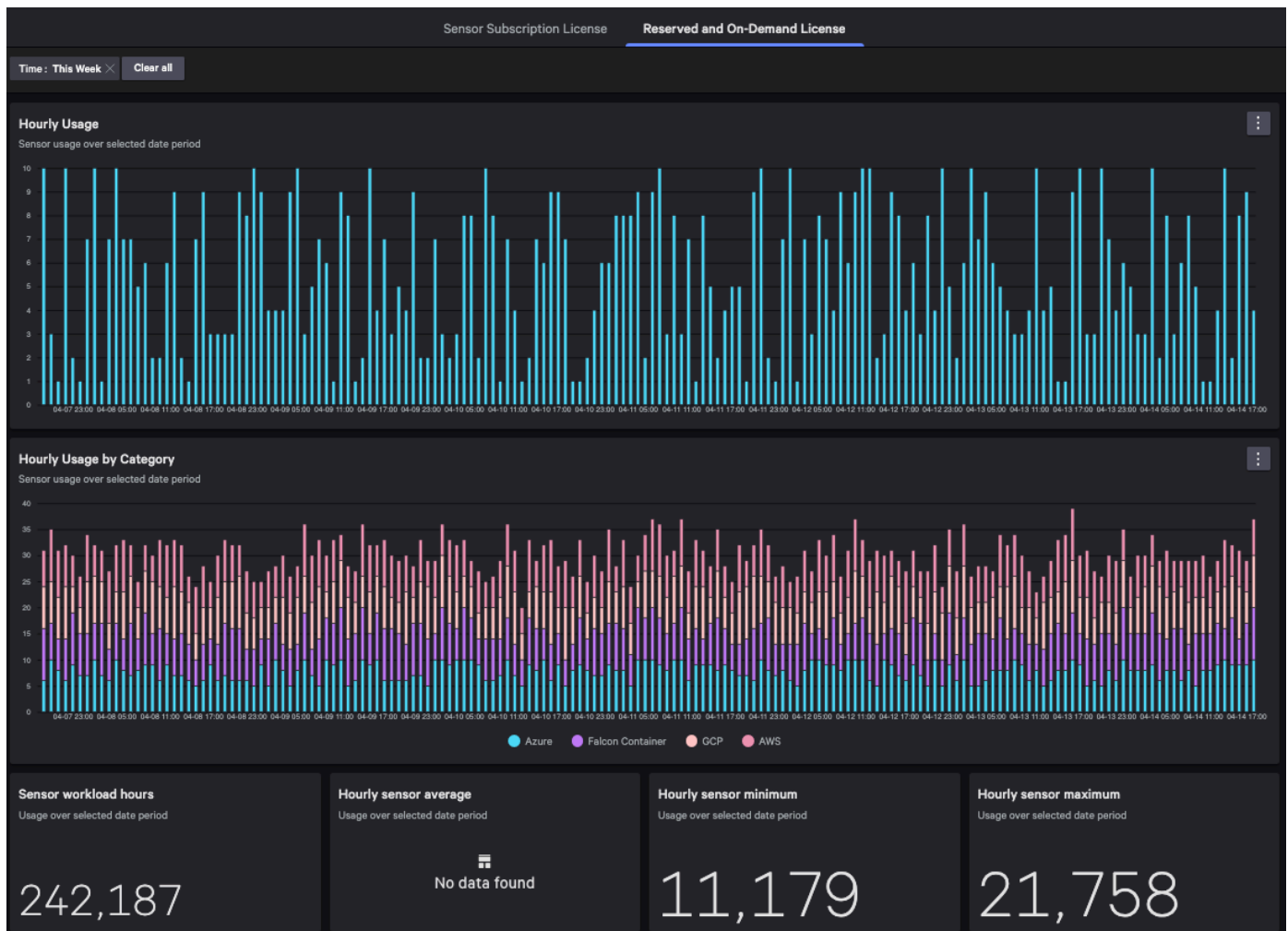
Section	Description and usage
Total usage by endpoint	The 4-week average sensor usage across all endpoint types for this CID.
Public cloud usage by endpoint	The 4-week average sensor usage across public cloud endpoints for this CID.
Server usage by endpoint	The 4-week average sensor usage across server endpoints for this CID.
Workstation usage by endpoint	The 4-week average sensor usage across workstation endpoints for this CID.
4-week sensor usage	The average of the weekly sensor usage over the last 4 weeks shown by usage type.
Unique sensors by category	Usage over the last 4 weeks by category.
Total unique sensors by endpoint	The 4-week total sensor usage across all endpoint types for this CID. Compare this number to the 4-week sensor average to understand usage spikes.
Cloud unique sensors by endpoint	The 4-week total sensor usage across public cloud endpoints for this CID.

Falcon Management

Section	Description and usage
Server unique sensors by endpoint	The 4-week total sensor usage across server endpoints for this CID.
Workstation unique sensors by endpoint	The 4-week total sensor usage across workstation endpoints for this CID.

View usage with the Reserved and on-demand licenses tab

With the appropriate licensing and the Falcon Administrator role, you can access this dashboard by going to [Dashboards and reports > Billing > Annual usage](#) and then clicking Reserved and on-Demand License at the top of the window.



This table explains the sections of the page.

Section	Description and usage
Hourly Usage	The number of cloud sensors running each hour during the specified time period. Each colored status bar represents one hour and shows a split view to give you insight into your average usage and usage that's over the average. Hover over a color in a graph bar to see additional details.
Hourly Usage by Category	Same as Hourly Usage with the bars divided to show usage by category.
Sensor workload hours	The total number of cloud sensor usage hours for the specified time period.
Hourly sensor average	The average number of sensors running per hour over the specified time period.

Falcon Management

Section	Description and usage
Hourly sensor minimum	The fewest number of sensors running in an hour over the specified time period.
Hourly sensor maximum	The greatest number of sensors running in an hour over the specified time period.

View usage with the Sensor usage dashboard

The Sensor usage dashboard provides a centralized view of sensor activity across your environment. Usage is broken down across 6 sensor categories in interactive line graphs to help you navigate and visualize your metrics more intuitively. This data can help you track current usage, better understand the usage trends of your hosts over time, and optimize your licensing allocation and management.

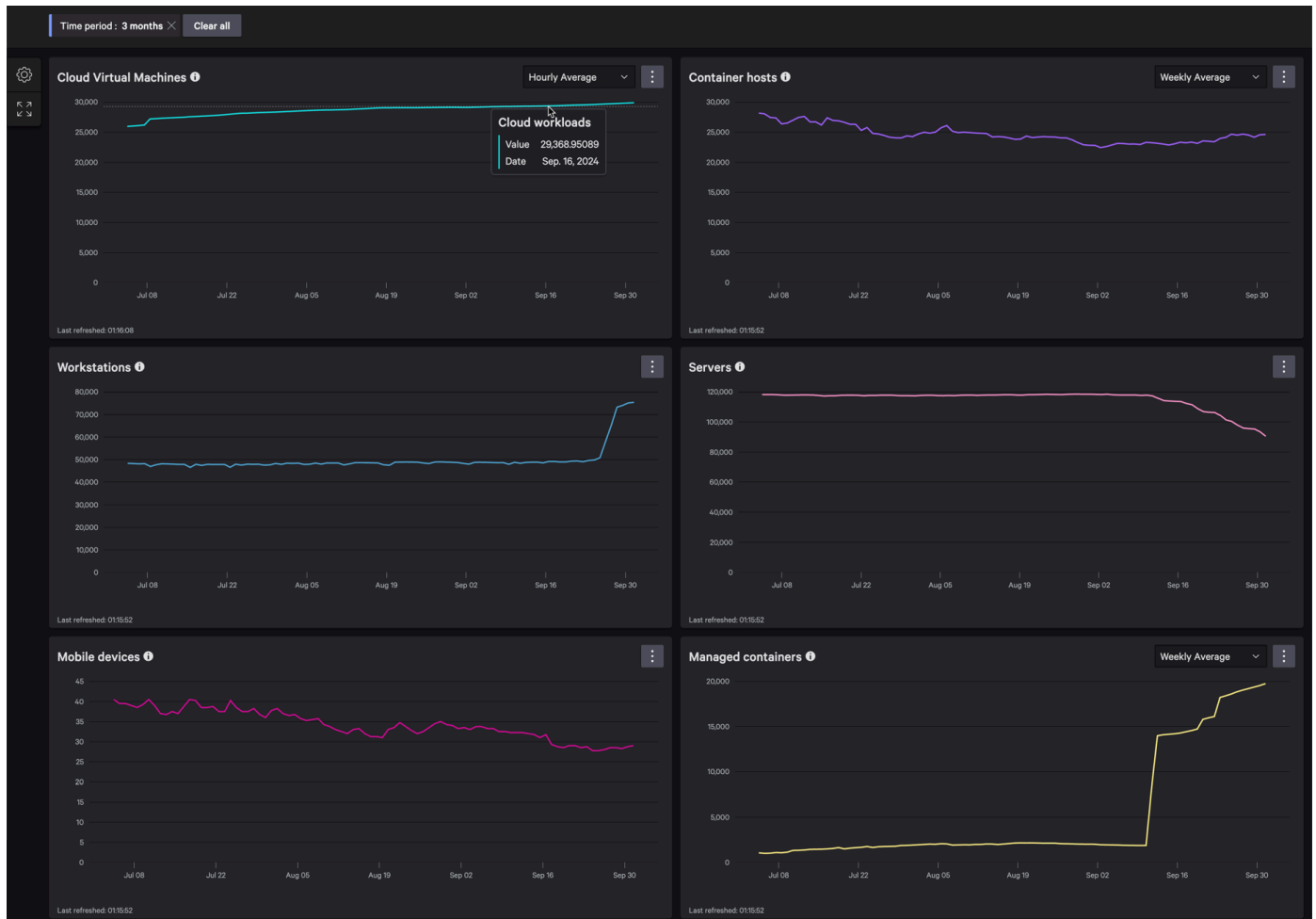
You can also access this data using the CrowdStrike API. For more info, see [Sensor Usage APIs](#).

The Sensor usage dashboard has these additional requirements:

- Roles:
 - Default roles: Billing Dashboard Admin
 - Custom role permissions:
 - Permission group: Manage Billing
 - Permission: View usage dashboards
- Contact your CrowdStrike account representative to enable these elements of this dashboard:
 - Hourly usage data: View hourly usage data for Cloud virtual machines, Container hosts, and Managed containers.
 - Usage data aggregation: Get aggregated usage data in multi-CID (non-Flight Control) accounts.
Note: Falcon Flight Control parent CIDs automatically receive aggregated child CID data.

To access the Sensor usage dashboard, go to [Dashboards and reports > Billing > Sensor Usage](#).

Note: Data is updated daily.



The dashboard provides you with these insights and options:

Falcon Management

Item	Description
Default data	See the average weekly sensor count over the previous 28 days by sensor category.
Sensor categories	Usage data is broken across these 6 categories: • Cloud virtual machines: Non-container-based AWS, Azure, Oracle (OCI) and Google Cloud public clouds. • Container hosts: Public clouds with containers and servers with containers • Managed containers: LUMOS • Mobile devices: Android and iOS devices • Servers: Non-container-based Windows servers, Linux servers, Domain Controllers, private clouds, and public clouds other than AWS, Azure, OCI, and Google Cloud • Workstations: Windows and macOS desktop and laptop machines
Interactive line graph	View usage trends over the selected time period. Hover over points in the chart to see data for specific days.
Time period	Choose from different time period presets to view data for the last 30 days, 3 months, 6 months, or 13 months.
Hourly data	In Cloud virtual machines, Container hosts, and Managed containers, use the dropdown menu to switch your view to the average hourly sensor count. Note: You might need to contact your CrowdStrike account representative to enable hourly usage data for your CID.
Export	Export a sensor category's usage data as a downloadable CSV or JSON file from the Open menu :.
Falcon Flight Control and multi-CID support	View aggregated usage data for all CIDs in the account. Note: If you belong to a multi-CID account and don't have Falcon Flight Control, you might need to contact your CrowdStrike account representative to enable this feature.

View POV usage and licensing data

View proof of value (POV) usage and licensing data for your environment in your Sensor subscription license and Reserve and on-demand license dashboards when you are in an active POV trial period. You can compare and anticipate usage trends and manage licensing for your environment with POV data.

To view POV data in your billing dashboards, go to either [Dashboards and reports > Billing > Sensor subscription licenses](#) or [Dashboards and reports > Billing > Reserve and on-demand licenses](#) and enable POV view. Your POV view expiration date is displayed in MM/DD/YY format. POV trial periods expire in 90 days by default unless specified otherwise.

Note: In POV view, existing sensor usage data might shift to different licenses depending on your subscriptions.

Tip: When POV view is enabled, click [View sensor subscription dashboard](#) or [View reserve/on-demand dashboard](#) to quickly switch between Sensor subscription license and Reserve and on-demand license dashboards.

Falcon Flex

Learn about Falcon Flex and how to view your Flex Pool details and active modules.

Overview

Falcon Flex is a program that allows you the flexibility and scalability to buy CrowdStrike product licenses without committing to specific quantities. You use the funds in your Flex Pool to easily adopt new modules, streamlining the buying process. You can activate and deactivate modules, minimizing lengthy procurement cycles and legal reviews associated with traditional licensing models. With Falcon Flex:

- Choose which security modules you need
- Add and remove modules as your needs change
- Pay only for the modules that you use
- Avoid paying for unnecessary features

View all active subscriptions, as well as their status and history, from a single, unified dashboard within the Falcon console. For more info, see [Dashboard](#).

Understanding your Flex commitment

Your Flex commitment is a prepaid balance that you commit to spend over your contract term. It consists of:

- Modules and bundles activated at the start of your contract
- Your Flex balance

Each time you activate a module or a bundle after your start date, the money spent comes from your Flex balance. You can track your Flex commitment spending and amount remaining using the Falcon Flex Dashboard. For more info, see [Dashboard sections and widgets](#).

Dashboard

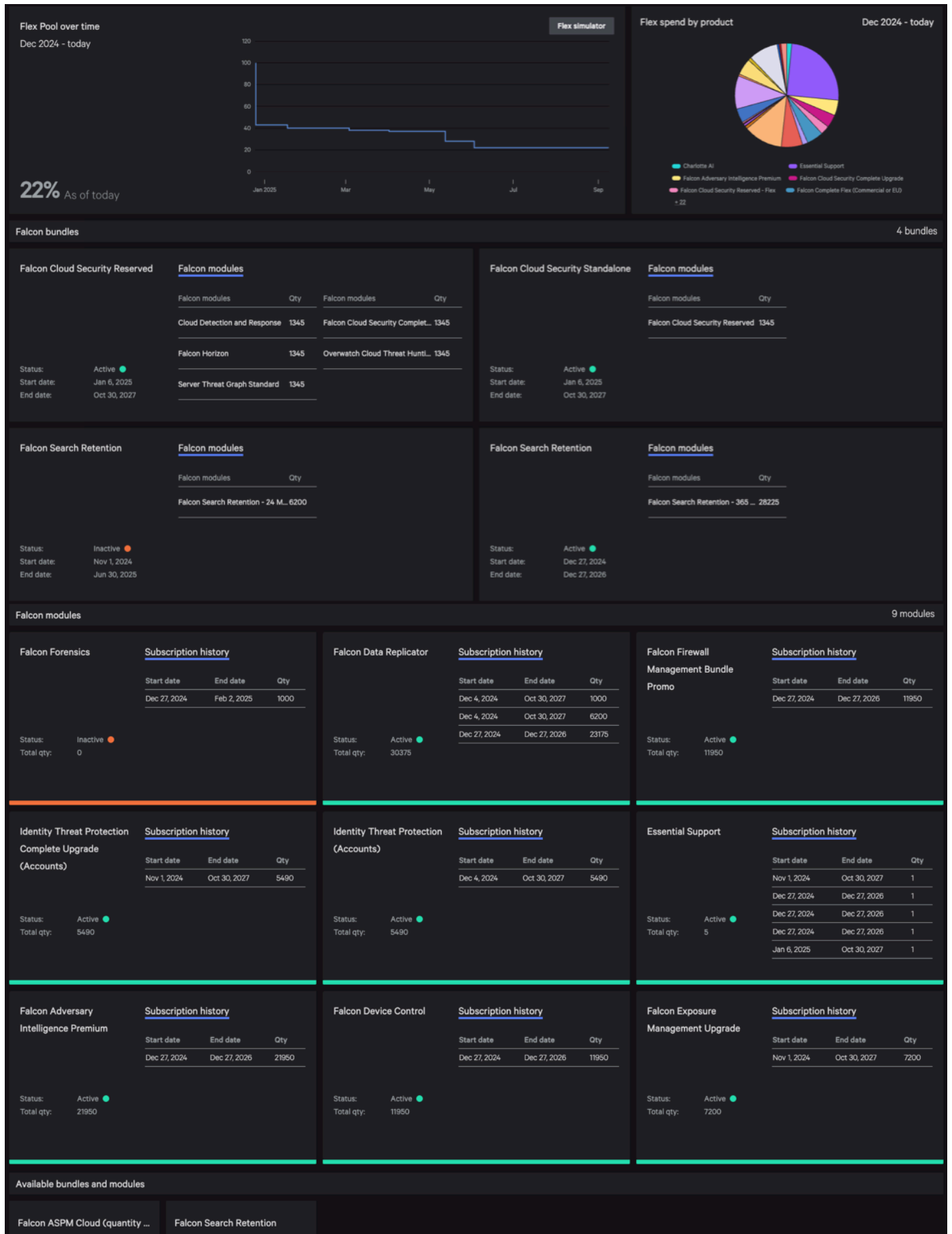
The Falcon Flex Dashboard provides a centralized view of all active modules, their status, and history.

With the Falcon Flex Dashboard, you can view:

Falcon Management

- A burndown chart of the percentage of funds remaining in your Flex commitment
- Your historical and projected spending trends
- The distribution of your Flex spending across products
- The status and history of your subscriptions
- Modules within your contract that are available for activation

To view the dashboard, in the Falcon console, go to Dashboards and reports > Billing > Falcon Flex .



Falcon Management

Requirements

Subscription: Any subscription for customers enrolled in Falcon Flex

Note: If you belong to a multi-CID account and don't have Falcon Flight Control, you might need to contact your CrowdStrike account representative to enable the dashboard for your CID. For more info about Falcon Flight Control and multi-CID accounts, see [Falcon Flight Control](#) and [Multi-CID Support](#).

Default roles: Falcon Administrator, Falcon Complete Administrator, Billing Dashboard Admin

CrowdStrike clouds: Available in US-1, US-2, EU-1, and US-GOV-1

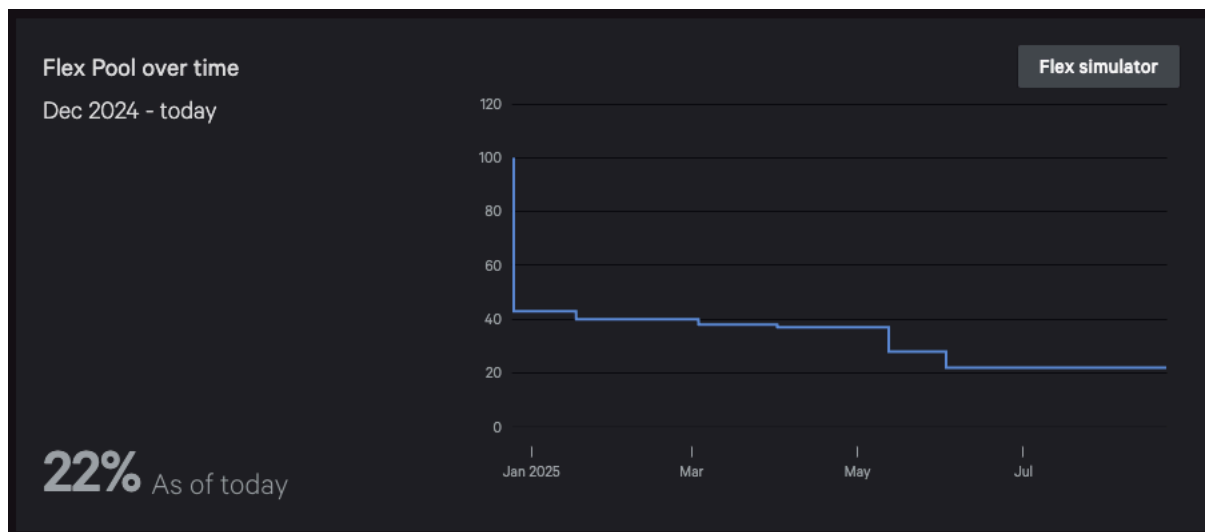
Dashboard sections and widgets

The Falcon Flex Dashboard is divided into multiple sections and widgets that allow you to track usage and view information about your Flex account.

Flex Pool over time

This widget contains a burndown chart showing funds remaining in your Flex account, represented in percentages. This chart shows how much of your Flex commitment has been spent from product activations.

The chart begins with your initial Flex commitment, shown as 100%, and each product activation deducts from this balance. Hover over a point in the chart to see the exact date and percentage of remaining funds.



Flex simulator

Use the Flex simulator tool to plan your Flex pool spending. With this tool, you can:

- View your historical and projected spending trends.
- Estimate the impact of activating modules at different times throughout your contract period so that you can plan when to activate new modules.
- Create custom simulations to plan how to spend your remaining Flex pool funds by choosing from different modules and adding license quantities and unit costs as needed. Based on your selections, the Flex Pool over time burndown chart dynamically updates to show your historical and projected Flex pool consumption trends as percentages of your total Flex commitment.



1. In the Flex Pool over time widget, click Flex simulator.
2. Click Add Module.

Falcon Management

3. From the Modules dropdown menu, select a module. You can also enter a custom module name and click Add to add it to the dropdown list.
4. The Unit field supports a variety of units of measurement. Enter a unit quantity based on the module type that you selected. For example:
 - a. For Next-Gen SIEM modules, enter the amount of GB.
 - b. For Identity Threat Protection, enter the number of accounts.
 - c. For endpoint-related modules, enter the number of endpoints.
5. In the Unit cost (\$) field, enter the price per module.
6. In the Activation date column, use the calendar widget to select an activation start date. Today's date is selected by default.
7. Optional. Click Add Module to add more modules.
8. In the Display column, disable the toggle next to each module you don't want to appear in the Flex Pool over time burndown chart.

Note: Your changes persist when you exit the Flex simulator dialog and go to other pages within the Falcon console and even after your session expires or you log out.

Export a Flex simulator report

After you create a Flex spending simulation using the Flex simulator tool, you can export the results as a report. This report contains all of the data shown in the Flex simulator, including the Flex Pool over time burndown chart.

1. In the Flex simulator dialog, click Open menu .
2. Select an export format option:
 - o Export PDF
 - o Export CSV
3. Follow the on-screen steps to save the exported report to your device.

Flex spend by product

This widget is a pie chart illustrating how your Flex commitment is allocated across different modules, helping you identify which modules consume the largest portion of your Flex commitment. Hover over a pie chart section to see the allocation percentage for that module.



Falcon bundles

This section displays a comprehensive view of licenses within bundles, including their Status (Active or Inactive) and their activation start and end date.

Falcon modules

This section displays the history of your Flex subscriptions, including their Status (Active or Inactive), their activation start and end date, and the quantity of licenses purchased.

Available bundles and modules

This section displays the names of modules and bundles that are available to activate in your Flex account. Please contact your CrowdStrike sales representative for module activation. Note: This section is only shown if you have inactive bundles or modules on your Falcon Flex rate card that were not part of Day-1 Activation.

Account Settings

IP Allowlist Management

Help ensure your account is only accessed from specific networks by configuring your IP allowlist to restrict access to specific IP addresses.

Overview

Define a list of IP addresses that are allowed to access your Falcon account. By default, user access is not limited by IP address. You can configure the IP allowlist to restrict access to specific IP addresses and help ensure your account is only accessed from specific networks. When a user attempts to sign in through the Falcon console or the CrowdStrike API, their IP address is evaluated against the allowlist. Access from unlisted IP addresses is denied.

Falcon Management

Requirements

Roles:

- Falcon Administrators can view the IP allowlist page and create and manage IP groups.

IP addresses:

- Your trusted company network egress IP must be configured with a static IP or static IP range.
- The IP allowlist feature works only with public IPv4 addresses. Private and IPv6 addresses are not supported.

Third-party application integrations:

- To enable IP allowlisting in an integrated third-party application accessing the CrowdStrike API (such as a [Partner Integration application](#)), the network IP range where the third-party app is running must be added to an IP group.

Falcon Flight Control

- IP enforcement occurs when a user signs in to their home CID (customer ID). IPs are not evaluated when switching between CIDs.

Understanding the IP allowlist

In the IP Allowlist ([Host setup and management](#) > [Falcon users](#) > [IP Allowlist Management](#)), you can define the IP addresses that have permission to access your account. By default, the IP Allowlist is empty, so all IP addresses are allowed. You can restrict access by configuring the allowlist in IP groups that contain one or more individual IP addresses and CIDR ranges. Each IP group specifies an access type that determines whether the listed IP addresses and CIDRs can access your account through the Falcon console UI or CrowdStrike API. After an IP group is created, it must be turned on before access restrictions begin. Falcon enforces any enabled IP group in your IP allowlist and blocks access from unlisted IP addresses and CIDRs.

You can use the IP allowlist to:

- Specify a range of IP addresses to allow Falcon console access from devices on your company network.
- Grant API access to IPs for your partner applications [integrated through the CrowdStrike Store](#).

You can create any number of IP groups and turn them on and off to meet your needs. You can also edit your IP groups and delete any IP groups that you no longer need. An [audit log](#) provides a history of changes made to your IP allowlist groups.

Note:

- IP Allowlists are controlled separately by CID.
- The IP allowlist feature works with individual public IPv4 addresses or ranges using CIDR notation. Private and IPv6 addresses are not supported.
- IPs are not checked if the IP allowlist is empty or if no configured IP groups are turned on.
- IP address blocking is not available.

Managing IP allowlist groups

Viewing your IP groups

View a full list of your CID's configured IP groups from the IP Allowlist page ([Host setup and management](#) > [Falcon users](#) > [IP Allowlist Management](#)). Each IP group in the list includes the following attributes:

- Name: The user-defined IP group name.
- Description: An optional description to define the group up to 500 characters in length. Hover to view longer descriptions in full.
- IP range: The individual IP addresses and CIDRs contained in the group. Hover to view longer IP lists in full.
- Access type: The type of access (API or UI) granted to IPs in the group.
- Status: The IP group's current status: On (active) or Off (inactive). Only IP groups with an On status will be used in authorizing access.
- 3 dot menu: Opens options to edit or delete the IP group.

Creating an IP group

Create an IP group to grant Falcon console or API access to specific IP addresses and CIDRs. IP groups are created in a disabled state and must be manually turned on for IP enforcement to begin. Falcon starts enforcing an IP group approximately 30 minutes after it's turned on.

- On the IP Allowlist Management page ([Host setup and management](#) > [Falcon users](#) > [IP Allowlist Management](#)), click Create IP group.
- Specify a name for the group up to 150 characters long. Alphanumeric characters and spaces are accepted. Special characters are not supported.
- Optional. Add a short description about the IP group up to 500 characters in length.
- Choose the type of access to allow IPs in the group. Select API, UI, or both.
- In the IP range field, enter an individual IPv4 address (such as 50.0.0.0) or a CIDR range (such as 50.0.0.0/8) per line. Wildcards are not supported.
- To add another individual IP address or CIDR, click Add another IP range. Repeat this step until all IP addresses and CIDRs are added to the group.
- Click Create IP group.
- Optional. To begin enforcement of the IP group, click the Status toggle On. Allow up to 30 minutes for enforcement to begin after toggling on the IP group.

Falcon Management

Turning an IP group on or off

To start or stop enforcement of an IP group, you can turn it on and off from the IP Allowlist Management page ([Host setup and management > Falcon users > IP Allowlist Management](#)). When an IP group is turned off, it's no longer used to restrict access. You can resume IP enforcement by turning the IP group back on.

Note:

- Changes to an IP group are applied immediately but may take up to 30 minutes to take effect.
- Incoming IPs are not checked if no IP groups are turned on.

1. Go to [Host setup and management > Falcon users > IP Allowlist Management](#) .
2. Click the Status toggle on the IP group to turn it On or Off.

Editing an IP group

You can modify an existing IP group's name, description, and access type as well as add, remove, or edit individual IP addresses or CIDRs. Note that changes to an IP group are applied immediately but may take up to 30 minutes to take effect.

1. Go to [Host setup and management > Falcon users > IP Allowlist Management](#) .
2. Next to the IP group you want to edit, click Open menu  and select Edit IP group.
3. Modify the group settings as needed. For more info, see [Creating an IP group](#).
4. Click Update IP group.

Deleting an IP group

If you no longer need an IP group, you can delete it. Deleting an IP group permanently removes it from Falcon. If you want to temporarily suspend IP enforcement, you can turn an IP group off. For more info, see [Turning an IP group on or off](#).

1. Go to [Host setup and management > Falcon users > IP Allowlist Management](#) .
2. Next to the IP group that you want to delete, click Open menu  and select Delete IP group.
3. In the confirmation window, click Delete IP group.

Viewing the IP allowlist audit log

Each time an IP group is created, edited, or deleted, an audit log entry is recorded in Falcon. You can use the audit log to view a history of changes made to your configured allowlist IP groups along with information about the activity that occurred.

1. Go to [Host setup and management > Falcon users > IP Allowlist Management](#) and click See audit log.
2. On the Falcon UI Audit Trail page, the Service is automatically set to IP Allowlist Management and the Time range shows Last 14 days.
 - Use filters to refine the audit log results, such as by Action (the type of activity that occurred) or Time range.
 - In the Audit Details, see the history log and review details about changes made to your IP groups, including what change occurred to which IP group, when, and by whom. Click a column header to sort the log by that attribute.

SCIM Provisioning

Automate user identity provisioning and management from your identity provider.

Overview

Falcon supports integration with System for Cross-domain Identity Management (SCIM). Using the SCIM protocol, you can automatically provision, update, and deprovision users in the Falcon console directly from your identity provider.

Understanding SCIM

With SCIM, your organization's users are set up in your identity provider and then provisioned to Falcon. You configure an app integration in your identity provider that uses SCIM 2.0 for user provisioning, and then assign groups of users to the app to define who can access your CID in the Falcon console. SCIM provisions these groups in Falcon and links existing user accounts or creates a new user account for each group member. You can assign roles to provisioned SCIM groups in the Falcon console to give members access to resources.

After you set up SCIM provisioning, management of users and groups is done in your identity provider. Any changes that you make to users and groups in the identity provider automatically sync to Falcon using the SCIM protocol.

Supported provisioning features

A SCIM integration with Falcon supports these provisioning features:

Falcon Management

- Provision users: SCIM provisions users in Falcon based on assignment to the SCIM app integration in your identity provider
 - Group push: Groups assigned to the identity provider SCIM app and group members are automatically provisioned when pushed to Falcon. Newly provisioned SCIM groups are assigned the host group All hosts and are not provisioned with a role by default. Users provisioned through a group push are given the Falcon Console Guest role. You can add roles to a SCIM group to move group members to new roles designated by the group.
 - Individual users: Users assigned to the identity provider SCIM app individually are automatically provisioned in Falcon with the default Falcon Guest role and All hosts host groups setting. You can view these users in the Falcon console, but any users who are added to Falcon individually and aren't in a SCIM group are restricted to the default Falcon Guest role and All hosts host group assignments.
- Update user attributes: Updates to a user's first or last name made through the identity provider are also updated in Falcon.
- Deprovision users: Your identity provider can use SCIM to deactivate or delete users from Falcon.
 - The option to deactivate or delete users depends on the identity provider's capabilities.
 - When a user is deprovisioned, they're assigned the Falcon Console Guest role, their user status in Falcon is set to Inactive, and they can no longer sign in to the Falcon console.
 - A user is deprovisioned in Falcon when any of these circumstances occur:
 - The user is part of a group that is removed from the SCIM app integration, and the removed group was the user's only association with the SCIM app integration. A user is not deprovisioned if they are still assigned to the SCIM app or belong to another group.
 - The user is completely removed from the SCIM app integration in the identity provider. This includes removing the user from groups associated with the app and unassigning the user from the SCIM app integration.
 - The user is deactivated or removed from the identity provider.

Supported identity providers

Falcon supports SCIM integration with these identity providers:

- Okta
- Microsoft Entra ID
- PingOne
- PingFederate

SCIM groups

Falcon's implementation of SCIM uses groups to organize users that you are syncing to Falcon. Groups are used to map members to specific Falcon roles. They simplify user management, allowing you to control access rights for multiple users collectively.

You create custom groups of users in your identity provider and push them to Falcon from your SCIM app integration. When a group is pushed, it's automatically provisioned in Falcon and re-created as a SCIM group with the same name and all of the group's members. By default, new SCIM groups are provisioned with host group access to All hosts and with no assigned role. Falcon Cloud Security subscriptions are provisioned with cloud group access to All cloud assets and with no assigned role.

Role assignment

You can assign roles to your provisioned SCIM groups in the Falcon console to grant permissions to group members. Whenever new users are added to the group in the SCIM app integration, they are automatically granted the roles allocated to the group.

Notes:

- Users can belong to more than one SCIM group. If you have users who require various roles, you can add the user to the groups where those roles are assigned.
- Falcon identifies users by email address and does not create duplicate user accounts when existing users are added to multiple SCIM groups.
- You can only manage roles for SCIM group members at the SCIM group level. This does not apply to temporary roles. Even with SCIM enabled, you can assign temporary roles to individual users. Temporary roles cannot be assigned to groups. For more info, see [Use temporary roles to grant and revoke access](#).

SCIM base URL

The SCIM base URL is the API entry point that connects your identity provider to Falcon. Each CrowdStrike cloud uses a different SCIM base URL. You'll provide your cloud's base URL when configuring SCIM in your identity provider:

- US-1: <https://api.crowdstrike.com/scim/v2>
- US-2: <https://api.us-2.crowdstrike.com/scim/v2>
- EU-1: <https://api.eu-1.crowdstrike.com/scim/v2>
- US-GOV-1: <https://api.laggar.gcw.crowdstrike.com/scim/v2>
- US-GOV-2: <https://api.us-gov-2.crowdstrike.mil/scim/v2>

SCIM API key

SCIM integration uses an API key for authenticating provisioning requests from your identity provider to your Falcon CID.

You generate your CID's API key from the SCIM groups page in the Falcon console and use it to configure the SCIM app integration in your identity provider. This key is unique to your CID, and only one SCIM API key can be active at a time. For more info, see [Generate a new API key](#).

Falcon Management

Note: Whenever a new key is generated, the previous key becomes invalid and your SCIM integration connection is broken until the new key is added to your SCIM app integration. Provisioned users can continue to access and use Falcon; however, any changes to users and groups made in the identity provider will not sync to Falcon until the connection is re-established.

API key expiration

For security reasons API keys have a limited lifespan. A key is valid for the time period supported by your CrowdStrike cloud from the date it's generated:

- US-1, US-2, EU-1: 1 year
- US-GOV-1, US-GOV-2: 90 days

You can see the expiration date for your API key on the SCIM groups page in the Falcon console. To ensure uninterrupted SCIM provisioning, you must generate a new API key and add it to your SCIM app integration in the identity provider before the old one expires. For more info, see [Generate a new API key](#).

You can generate a new API key at any time and don't need to wait for the current key to expire to renew it. If your SCIM API key expires, your SCIM integration with Falcon breaks. If this happens, your provisioned Falcon users can continue to access Falcon and work normally. However, you cannot provision, deprovision, or update any users or groups from your SCIM app integration in the identity provider to Falcon until the connection is re-established.

API key expiration notifications

Falcon Administrators are notified by email about upcoming API expiration at the following times:

- 4 weeks before the key expires
- 1 week before the key expires

You can also see your API key's expiration date at any time in the Falcon console on the SCIM groups page.

Configuration mode

SCIM is initially enabled for your CID in a temporary configuration mode. This gives you time to set up and test your SCIM implementation without affecting the roles of your existing users.

While in configuration mode:

- You can assign groups to the SCIM app integration in the identity provider and the users are added in Falcon.
- You can create and push SCIM groups from your identity provider to Falcon.
- You can assign roles, host groups, and cloud groups to your SCIM groups in the Falcon console; however, these assignments are not granted to the SCIM group members until your SCIM integration is in production mode.
- You can manually update user accounts from the Falcon console.
- The roles, permissions, and settings in your CID's existing user accounts remain in effect.

When you exit configuration mode:

- Only users that are provisioned through SCIM are added to your CID in Falcon.
- You are no longer able to manage user accounts through the Falcon console.
- User accounts that existed in Falcon prior to enabling SCIM provisioning are handled as follows:
 - If the user account also exists in the identity provider SCIM app integration, the user accounts are merged and management is maintained through the identity provider.
 - If the user account does not exist in the identity provider SCIM app integration, the user account is assigned the Falcon Console Guest role.

Preview provisioned users and SCIM groups

While working in configuration mode, you can download a CSV or JSON file to preview how your users will be provisioned when you move to SCIM production mode. The preview report contains basic user account info and shows each user's current roles, host groups, and Flight Control user groups along with what those assignments will be when SCIM provisioning is enforced. You can use the report to ensure user attribute accuracy, confirm successful group provisioning, and verify users are being properly provisioned with the right permissions.

The preview report includes these data points for each of your users:

- First name: The user's first name
- Last name: The user's last name
- Email: The user's email address
- Assignment CID: The user's assigned Falcon CID
- Current Roles: The non-temporary roles currently assigned to the user
- New Roles: The roles that the user will be granted when SCIM provisioning is fully enabled
- Current Host Groups: The host groups currently assigned to the user
- New Host Groups: The host groups that the user will be assigned to when SCIM provisioning is fully enabled
- SCIM Groups: The SCIM groups that the user is assigned to
- Changed: Indicates whether any changes are identified between the user's current data and the new data

Falcon Flight Control Parent CID reports include these additional fields:

- Home CID: The user's assigned home CID
- Current FCTL Legacy User Groups: Any Flight Control user groups the user is currently assigned to
- New FCTL User Groups: The Flight Control user groups that the user will be assigned to when SCIM provisioning is fully enabled

Falcon Management

Falcon Cloud Security subscriptions include these additional fields:

- Current Asset Groups: The cloud groups currently assigned to the user
- New Asset Groups: The cloud groups that the user will be assigned to when SCIM provisioning is fully enabled

You can generate a preview report from the SCIM groups page in the Falcon console.

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Click the SCIM groups tab.
3. Click Preview.
4. Select CSV or JSON for the file format for your report.

When the report is ready, click Download. The report file is available for download for 24 hours.

Falcon Flight Control support

SCIM provisioning is supported in multi-CID accounts with Falcon Flight Control. In your identity provider, you configure a distinct SCIM app integration for each CID in your Flight Control deployment where you want to use SCIM provisioning. This allows you to control provisioning, deprovisioning, and management of users homed in a CID. In each SCIM app integration, you assign the CID's home users and push them to Falcon in groups. Then, similar to SCIM-enabled, non-Flight Control CIDs, you can manage role, host group, and cloud group assignments from the Falcon console.

From the parent CID, you can continue to control access at a more granular level with Flight Control user groups. However, when SCIM is fully enabled, you assign a user group to a SCIM group instead of to users individually. All users in the SCIM group are granted the access permissions defined in the user group.

Set up SCIM provisioning

This section gives an overview of the prerequisites and tasks you must complete to set up and start using SCIM. For details, see the linked sections.

Prerequisites

- Roles: To set up SCIM, you need these levels of access:
 - The Falcon Administrator role in your CID
 - An admin account in your identity provider
- SAML-based Single Sign-On (SSO) must be enabled for your CID. For info, see [Single Sign-On \(SSO\) for Falcon](#).

Basic workflow

Important: Ensure that you complete all steps in this section in order.

Setting up a SCIM integration includes these general steps:

1. Set up SSO.
2. Add the SCIM feature to your Falcon CID.
3. Get your SCIM base URL and API key.
4. Configure SCIM in your identity provider.
5. Assign roles, host groups, and cloud groups to your provisioned SCIM groups.
6. Preview provisioned users and SCIM groups.
7. Transition from configuration mode to running SCIM in production.

Step 1: Set up SSO

To use SCIM, your CID must have SAML-based SSO configured and fully enabled with your identity provider. For more info, see [Single Sign-On \(SSO\) for Falcon](#).

Step 2: Add the SCIM feature to your Falcon CID

Contact support using the [CrowdStrike Customer Center](#) and request to add the SCIM feature to your CID in configuration mode.

Step 3: Get your SCIM base URL and API key

Get the SCIM base URL for your cloud and generate your CID's SCIM API key. You'll enter these when configuring your SCIM app integration.

SCIM base URL

Use the SCIM base URL for your CrowdStrike cloud:

Falcon Management

- US-1: <https://api.crowdstrike.com/scim/v2>
- US-2: <https://api.us-2.crowdstrike.com/scim/v2>
- EU-1: <https://api.eu-1.crowdstrike.com/scim/v2>
- US-GOV-1: <https://api.laggar.gcw.crowdstrike.com/scim/v2>
- US-GOV-2: <https://api.us-gov-2.crowdstrike.mil/scim/v2>

SCIM API key

Generate your CID's API key from the SCIM groups page in the Falcon console. For more info about API keys and SCIM, see [SCIM API key](#).

1. Go to [Host setup and management > Falcon users > User management](#).
2. Click the SCIM groups tab.
3. Click Generate API Key.

Note: In Falcon Flight Control parent CIDs, select the CID you'd like to generate the API key for from the list provided.

4. Copy the API key and store it in a secure location. You'll use it when configuring your SCIM app integration in your identity provider. Note: The API key only appears once and is no longer visible after the credential window closes.

Step 4: Configure SCIM in your IdP

When setting up SCIM, you install and configure an app integration to connect your identity provider to your Falcon CID. The SCIM provisioning configuration process varies by identity provider. To help you get started, we provide basic setup guides for each of our supported identity providers. You can find detailed SCIM implementation info in your identity provider's documentation.

SCIM provisioning setup guides:

- [Set up SCIM provisioning with Okta](#)
- [Set up SCIM provisioning with Microsoft Entra ID](#)
- [Set up SCIM provisioning with PingOne](#)
- [Set up SCIM provisioning with PingFederate](#)

Step 5: Assign roles, host groups, and cloud groups to your provisioned SCIM groups

You can grant roles and assign host groups and cloud groups to your provisioned SCIM groups in the Falcon console. All group members inherit the roles, host groups, and cloud groups assigned to the SCIM group. For more info, see [Manage SCIM group roles, host groups, and cloud groups](#).

Important: If you want to assign roles, host groups, and cloud groups, this step must be completed before [Step 7. Transition from configuration mode to running SCIM in production](#). If you skip this step, all Falcon users will default to the Falcon Guest role.

Step 6: Preview provisioned users and SCIM groups

Verify your SCIM group mapping configuration with the SCIM preview feature. For more info, see [Preview provisioned users and SCIM groups](#).

Step 7. Transition from configuration mode to running SCIM in production

When you're ready to safely switch to SCIM production mode, contact Support with our [CrowdStrike Customer Center](#). As soon as your CID transitions to full SCIM provisioning, your users are provisioned in Falcon with the permissions shown in the preview report.

Manage provisioned SCIM groups and users

When running SCIM in production, management of users and groups is maintained in the identity provider. To manage permissions granted to group members, you can assign roles, host groups, and cloud groups to provisioned SCIM groups in the Falcon console.

View provisioned SCIM groups in the Falcon console

Groups synced from your identity provider SCIM app integration are added as SCIM groups in Falcon. You can view these groups and assign them roles, host groups, and cloud groups from the SCIM groups page in the Falcon console to grant group members access to resources.

To access the SCIM groups page, go to [Host setup and management > Falcon users > User management](#) and click the SCIM groups tab. You must have the SCIM feature turned on in your CID for this page to appear.

Falcon Management

- Each SCIM group in the list includes these details:
 - SCIM group name: The name of the SCIM group, as defined in the identity provider.
 - Access last modified: The date and time the SCIM group was last modified in Falcon.
 - User last synced: The date and time of the most recent user synchronization.
 - User count: The number of active users assigned to the SCIM group.
 - Home CID (Falcon Flight Control parent CIDs only): The CID where the SCIM group was created. In Falcon Flight Control parent CIDs, the SCIM Groups page includes SCIM groups homed in child CIDs.
 - Roles: The user roles assigned to the SCIM group. Roles are granted to all SCIM group members.
 - Host groups: The host groups assigned to the SCIM group. By default, a new SCIM group is assigned All hosts.
 - Cloud groups: The cloud groups assigned to the SCIM group.
- Sort the list of SCIM groups at the column level by different criteria in ascending or descending order. By default, SCIM groups are ordered alphanumerically by name.
- Click a group in the list to open the details panel and view more information about the SCIM group, including group metadata and assigned roles, host groups, and cloud groups. Flight Control parent CIDs also show associated Flight Control user groups and a breakdown of data for each CID that the SCIM group has access to.

Click a group's Open menu : and select View details page for more detailed information about the SCIM group. From this view, you also can see the users that are members of the group and manage roles and group assignments.

Host setup and management

User management > SCIM Groups

Q Search

Colossal Dynamic Corp

Users (12)

SCIM groups (4)

Key expires: Oct. 7, 2025

Generate API key

SCIM group na...	Access last mo...	User last synced	User count	Roles	Host groups	Reporting
Admins	Oct. 16, 2024 07:35:51	Oct. 16, 2024 07:35:51	2	Falcon Administrator	All hosts	Group details Name Reporting Last modified Oct. 10, 2024 01:59... Modified by 2b462b5845d3b5845... Users last synced Oct. 10, 2024 01:59... Home CID Colossal Dynamic Corp User count 5 Access per CID Colossal Dynamic Corp (Home CID) Roles Scheduled Report Admin Dashboard Admin Host groups Data 3
Analysts	Oct. 8, 2024 23:48:35	Oct. 8, 2024 23:48:35	2	Falcon Analyst	All hosts	
Devs	Oct. 10, 2024 01:41:39	Oct. 10, 2024 01:41:39	2	App Developer	Eng 1	
Reporting	Oct. 10, 2024 01:59:41	Oct. 10, 2024 01:59:41	5	Dashboard Admin, ...	Data 3	

4 results (1-4 shown)

Items per page 50

Page 1 of 1

See details page

Manage SCIM group roles, host groups, and cloud groups

You can grant roles and assign host groups and cloud groups to your provisioned SCIM groups from the Falcon console. All users in the group are automatically granted the roles, host groups, and cloud groups assigned to a SCIM group.

Notes:

- Role, host group, and cloud group assignments granted to users through SCIM groups do not take effect until your SCIM integration is fully enabled in production mode.
- A new SCIM group is provisioned in Falcon with no assigned role and with host group and cloud group access to All hosts.
- A new user is provisioned in Falcon with the Falcon Console Guest role and host groups and cloud groups set to All hosts. These defaults change when the roles, host groups, and cloud groups in the user's assigned SCIM groups change.
- When users are added to or removed from a provisioned SCIM group in the identity provider, they gain or lose the roles granted to the group.
- Roles, host groups, and cloud groups can only be assigned to SCIM groups. Assignment to individual users is not supported, unless you assign a temporary role.
- For more info about cloud groups, see Controlling access to cloud assets and images (Legacy).

Requirements

Host group requirements:

Falcon Management

- Subscription: All subscriptions
- Default roles: Management of host groups is handled by cross-subscription default roles. For more info, see [Cross-subscription default roles](#).
- Clouds: Available in all clouds

Cloud group requirements:

- Subscription: Falcon Cloud Security
- Default roles: Falcon Administrators can manage provisioned SCIM groups and users in the Falcon console
- Clouds: Available in all clouds

Assign roles to a SCIM group

1. In the Falcon console, go to [Host setup and management > Falcon users > User management](#) .
2. Select the SCIM groups tab.
3. Click the Open menu : on the SCIM group that you want to assign roles to.
4. Click [View details](#) page.
5. Click [Expand](#) next to the CID name.
6. Click [Assign roles](#) in the Roles section.
7. Add one or more roles from the list.
8. Click [Assign](#).

View a SCIM group's assigned roles

1. In the Falcon console, go to [Host setup and management > Falcon users > User management](#) and click the SCIM groups.
2. You can see a group's assigned roles in these places:
 - SCIM groups list: The Roles column shows roles assigned to the group. Hover over the list to see roles that don't fit in the window.
 - Summary panel: Click a SCIM group row to open the summary panel. Then expand the CID section to view the assigned roles.
 - SCIM group details page:
 - Click the SCIM group's Open menu : and select [View details](#) page.
 - On the SCIM group details page, click [Expand](#) next to the CID name to see the roles assigned to the group.

Assign host groups to a SCIM group

1. In the Falcon console, go to [Host setup and management > Falcon users > User management](#) .
2. Click the SCIM groups tab.
3. Click the Open menu : on the SCIM group that you want to assign host groups to.
4. Click [View details](#) page.
5. Click [Expand](#) next to the CID name.
6. In the Host groups section, click [Assign host groups](#).

Note: If [Assign host groups](#) is disabled, click [Remove](#) to remove access to all hosts and enable individual host group assignment.
7. Select one or more host groups from the list of available options, and then click [Assign](#).

Assign cloud groups to a SCIM group

1. In the Falcon console, go to [Host setup and management > Falcon users > User management](#) .
2. Click the SCIM groups tab.
3. Click the Open menu : on the SCIM group that you want to assign cloud groups to.
4. Click [View details](#) page.
5. Click [Expand](#) next to the CID name.
6. In the Cloud groups section, click [Assign cloud groups](#).

Note: If [Assign cloud groups](#) is disabled, click [Remove](#) to remove access to all hosts and enable individual cloud group assignment.
7. Select one or more cloud groups from the list of available options, and then click [Assign](#).

View a SCIM group's assigned host groups and cloud groups

1. In the Falcon console, go to [Host setup and management > Falcon users > User management](#) .
2. Click the SCIM groups tab. You can see the host groups and cloud groups assigned to a SCIM group in these places:

Falcon Management

- SCIM groups list: The Host groups column shows the SCIM group's assigned host groups. Hover over the list to see host group names that don't fit in the window.
- Group details panel: Click the SCIM group in the list to open the group details panel. Then, expand the CID section to view the assigned host groups and cloud groups.
- SCIM group details page:
 - Click the SCIM group's Open menu : and select View details page.
 - On the SCIM group details page, click Expand next to the CID name to see the assigned host groups and cloud groups.

Add SCIM group users to Flight Control user groups

To manage access at a more granular level, Falcon Flight Control deployments can assign SCIM groups to user groups. When you assign a SCIM group to a user group, the permissions defined in the user group are granted to all SCIM group members.

User group management is only available from the Flight Control parent CID.

For more info about Flight Control user groups, see [Managing user groups](#) in our Falcon Flight Control documentation.

1. In the Falcon console, go to [Host setup and management > Falcon users > User management](#) .
2. Click the SCIM groups tab.
3. Click the Open menu : on the SCIM group that you want to assign to a user group.
4. Click View details page.
5. Click Expand next to the CID name.
6. Click Assign user groups n the User groups section.
7. Select one or more user groups from the list.
8. Click Assign.

Generate a new API key

Your SCIM app integration uses an API key for authenticating provisioning requests from your identity provider to your Falcon CID. This API key is generated in the Falcon console and added to your SCIM app integration in your identity provider.

Note: Generating a new API key immediately invalidates the old key and breaks your SCIM integration connection until the new key is added in your identity provider. Provisioned users can continue to access and use Falcon, however you cannot sync any changes from your identity provider to Falcon until the connection is re-established.

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Select the SCIM groups tab.
3. Click Generate API Key.

Note: In Falcon Flight Control parent CIDs, select the CID you'd like to generate the API key for from the list provided.

4. Copy the API key and store it in a secure location. The API key only appears once and is no longer visible after the credential window closes.
5. Update SCIM app integration in your identity provider with the new key. For more info, see your identity provider's documentation.

Set up SCIM provisioning with Okta

Use the SCIM protocol to import user identities from Okta to your Falcon CID. We've provided a basic guide below to help you set up SCIM with Okta. For more detailed implementation info, see [Okta's official SCIM documentation](#):

- [Understanding SCIM](#)
- [Okta and SCIM version 2.0](#)

Prerequisites

Before getting started, ensure these prerequisites are met:

- Set up SSO with Okta for your CID
- Enable SCIM in configuration mode through the CrowdStrike Customer Center
- Get your SCIM base URL and API Key

Workflow process

The setup process includes these tasks:

1. [Create a SCIM app integration](#)
2. [Set up the SCIM connection](#)
3. [Configure provisioning options](#)
4. [Set user attribute mappings](#)
5. [Sync users and groups to Falcon](#)

Falcon Management

6. Management tips and integration limitations

Create a SCIM app integration

Set up an app integration that uses SCIM for automatic user provisioning.

Note for Falcon Flight Control accounts:

If your existing SAML app configuration manages SSO for users homed in multiple child CIDs, you must use option 2 and add a separate SCIM app for each child CID. Option 1 is only available for SAML apps configured to manage SSO for users homed in the same CID in Falcon.

There are 2 options available in Okta:

- Use an existing SAML app: If you already use Okta for SSO, you can enable and configure SCIM from your existing Falcon SAML app integration.

If you're using this option, skip to the next section: [Set up the SCIM connection](#).

- Add a new SCIM app: Configure a new Okta SCIM 2.0 app. For more info, see [Add a SCIM 2.0 app to Okta](#).

Add a SCIM 2.0 app to Okta

1. In the Okta Admin Console, go to Applications > Applications.
2. Click Browse App Catalog.
3. Search for SCIM 2.0 Test App (OAuth Bearer Token), and click Add Integration.
4. Optional. In General settings, replace the placeholder app name in the Application label with a name of your own.
5. Leave the rest of the options as-is and click Next.
6. In the Sign-On Options, leave the default SAML 2.0 and Advanced Sign-on Settings.
7. Under Credential Details, set the Application username format to Email.
8. Click Done.

Set up the SCIM connection

Set up synchronization between your app integration and your Falcon CID. To complete the steps in this section, you need your SCIM base URL and the API key that you generated in the Falcon console. For more info, see [SCIM base URL](#) and [SCIM API key](#).

Set up connection to an Okta SCIM app

1. In your app integration, select the Provisioning tab.
2. Click Configure API integration.
3. Select the Enable API Integration checkbox.
4. In the SCIM 2.0 Base URL field, enter the SCIM base URL for your CrowdStrike cloud. For the URLs, see [SCIM base URL](#).
5. In the API Token field, enter your CID's API key that you generated in the Falcon console as the OAuth Bearer Token value.
6. Click Test API Credentials. This checks your base URL and API key to ensure a valid connection between Okta and your Falcon CID. If you receive an error, make sure your base URL and API key are correct and try again.
7. Click Save.

Set up connection to a SAML app

1. In your app integration, select the General tab.
2. Go to App Settings and click Edit.
3. Next to Provisioning, select Enable SCIM provisioning.
4. Click Save.
5. On the Provisioning tab, go to SCIM Connection and click Edit.
6. Provide the following information:
 - SCIM connector base URL: Enter the SCIM base URL for your CrowdStrike cloud. For the URLs, see [SCIM base URL](#).
 - Unique identifier field for users: Enter userName.
 - Supported provisioning actions: Select Push New Users, Push Profile Updates, and then Push Groups.
 - Authentication Mode: Select HTTP Header.
 - HTTP Header Authorization, Bearer Token: Enter your CID's API key that you generated in the Falcon console.
7. Click Test Connector Configuration. This checks your base URL and API key to ensure a valid connection between Okta and your Falcon CID. If you receive an error, make sure your base URL and API key are correct and try again.
8. Click Save.

Falcon Management

Configure provisioning options

Next, configure SCIM features for provisioning users and groups from Okta to Falcon.

1. Select the Provisioning tab of the app.
2. Select To App and then click Edit.
3. Select the checkboxes to enable these options:
 - Create Users
 - Update User Attributes
 - Deactivate Users
4. Click Save.

Set user attribute mappings

After configuring provisioning options, you must set Attribute Mappings. Keep only these 3 fields that you can sync with Falcon:

- Username (email)
- Given name (first name)
- Family name (last name)

Delete other attributes from the list. You cannot sync these with Falcon.

Sync users and groups to Falcon

After configuring the provisioning settings, follow these steps to sync users and groups with Falcon.

Notes:

- To sync groups of users to Falcon from Okta, the users need to be assigned directly to the SCIM app, and the group needs to be pushed. You must create separate groups in Okta for each of these purposes:
 - App Assignment: Create a group for assigning users to the SCIM app. Assigning a group to the SCIM app adds the users in that group individually in Falcon. The group itself is not added to Falcon.
 - Group Push: Create a group of users that you want to push to Falcon. A pushed group and its members are replicated in Falcon. You can assign roles, host groups, and cloud groups to your pushed SCIM groups in Falcon.
 - Using the same group for assignments and group push in the SCIM app integration is not supported by Okta and might result in error. For more info, see [Okta's documentation about App assignments and Group push](#) and [Using the Same Group for Application Assignment and Group Push](#).
1. On the Assignments tab of the app, click Assign and select Assign to Groups.
 2. Click Assign next to each group that you want to assign to the app.
 - A user account is created in Falcon for each user in the assigned groups.
 - If a user already exists in Falcon, a duplicate user account is not created.
 - An assigned group does not itself sync to Falcon. Only the group's users are synced.
 3. Click Done when finished.
 4. Go to the Push Groups tab, click Push Groups, and select Find groups by name.
 5. Search your existing Okta groups and select the group that you want to add to Falcon when it appears.
 6. Leave Push group members immediately selected if you want to immediately sync the group and its members to Falcon. If you turn off the automatic push, you can manually push your groups later.
 - Pushing a group re-creates the group in Falcon with the same name and all of the group's members.
 7. Click Save & Add Another to add more groups. When finished adding groups, click Save.
 - Syncing of users and groups is controlled by Okta and might take time to complete.

To verify that users and groups synced correctly, go to [Host setup and management > Falcon users > User management](#) and select the Users and SCIM groups tabs.

Management tips and integration limitations

There are a few management tips and limitations to keep in mind for your Okta SCIM integration with Falcon.

Okta user and group management

When SCIM is enabled, you manage your users and groups in Okta.

When you make these changes to your provisioned users and groups in Okta, they're reflected in Falcon:

Falcon Management

- Deactivating or deleting a user in Okta deactivates the user in Falcon and sets the user status to Inactive.
- Assigning a user to the SCIM app and adding them to a provisioned push group automatically adds the user to the corresponding SCIM group in Falcon with the roles, host groups, and cloud groups allocated to the group.
- Unassigning a user from the SCIM app deactivates the user in Falcon.
- Removing a user from a provisioned push group in Okta removes them from the corresponding SCIM group in Falcon.
 - The user loses the roles and permissions granted to them through the group.
 - If the user is not associated with any other provisioned SCIM groups, they are deactivated in Falcon and assigned the Falcon Guest role.
- Unlinking and deleting a push group from the SCIM app in Okta results in these actions:
 - Removes users from the group and deletes the SCIM group in Falcon
 - Users who were in the group lose the roles granted to the deleted SCIM group. However, the users are not deleted from the Falcon console.
 - Users in the group who are not associated with another SCIM group are deactivated in Falcon and can no longer sign in to Falcon. These users show an Inactive user status and are assigned the Falcon Guest role.
- Editing a user's first or last name in Okta syncs to Falcon.

Falcon does not support these SCIM features with Okta:

- Deleting users in Falcon. If a user is removed from a push group or the SCIM app, or if the user is deleted from Okta, they are deactivated in Falcon and no longer able to sign in.
- Importing users and groups from Falcon using Okta's import feature.
- Assigning Falcon user roles, host groups, and cloud groups.

Falcon user and group management

In the Falcon console, you can view your provisioned SCIM groups and users and manage these options:

- Assign roles to SCIM groups. All group members are granted the roles assigned to the group.
- Assign host groups and cloud groups to SCIM groups. All group members are given access to the host groups and cloud groups assigned to the SCIM group.

For more info, see [Manage SCIM group roles](#), [host groups](#), and [cloud groups](#).

Set up SCIM provisioning with Microsoft Entra ID

You can create an enterprise app integration in Microsoft Entra ID that uses SCIM for user provisioning. We've provided a basic guide to help you get set up. For more detailed info, see Microsoft's official SCIM documentation:

- [SCIM synchronization with Microsoft Entra ID](#)
- [How Application Provisioning works in Microsoft Entra ID](#)
- [SCIM provisioning tutorial: Getting started](#)

Prerequisites

Before getting started, ensure these prerequisites are met:

- [Step 1: Set up SSO](#)
- [Step 2: Add the SCIM feature to your Falcon CID](#)
- [Step 3: Get your SCIM base URL and API key](#)
- You must have an active Microsoft Entra ID enterprise subscription and administrator privileges in your account.

Workflow process

The setup process includes these tasks:

1. [Create a SCIM app integration](#)
2. [Connect your Falcon CID](#)
3. [Set user and group attribute mappings](#)
4. [Assign users and groups to your SCIM app integration](#)
5. [Turn on provisioning](#)
6. [Management tips and integration limitations](#)

Create a SCIM app integration

Each SCIM app integration in Entra ID is used for provisioning users and groups in a single Falcon CID. If you manage multiple CIDs, you must create a distinct app integration for each CID that will use SCIM provisioning.

1. In the Microsoft Entra Admin Center, go to [Applications > Enterprise applications](#).

Falcon Management

2. Click + New application.
3. Click + Create your own application.
4. Enter a name for your app.
5. Select Integrate any other application you don't find in the gallery (Non-gallery).
6. Click Create.

Connect your Falcon CID

Set up a connection between your Entra ID SCIM app integration and your Falcon CID. To complete the steps in this section, you need your SCIM base URL and the API key that you generated in the Falcon console. For more info, see [SCIM base URL](#) and [SCIM API key](#).

Note: Due to a known Microsoft issue, you must append the `aad0ptscim062020` feature flag to your SCIM base URL for your requests to be SCIM 2.0 compliant and work in Falcon. For more info, see [Microsoft's official documentation](#).

1. In your Entra ID SCIM app, go to Provisioning and click Get started.
2. Set the following provisioning properties:
 - o Provisioning Mode: Set to Automatic
 - o Tenant URL: Enter the SCIM base URL for your CrowdStrike cloud with the `?aad0ptscim062020` feature flag parameter appended to ensure SCIM compliance. For example, if your base SCIM URL is `https://api.crowdstrike.com/scim/v2`, enter this Tenant URL value: `https://api.crowdstrike.com/scim/v2/?aad0ptscim062020`
 - o Secret Token: Enter your CID's API key that you generated in the Falcon console.
3. Click Test Connection. This validates the connection between your app and your Falcon CID. If you receive an error, verify that your base URL and API key are correct and try again.
4. Click Save.

Set user and group attribute mappings

Set the attributes that are mapped from your SCIM app integration to the Falcon platform.

1. In your Entra ID SCIM app, go to Provisioning.
2. Expand Mappings and select Provision Microsoft Entra ID Users.
3. Under Target Object Actions, make sure Create, Update, and Delete are all selected.
4. In the Attribute Mappings list, delete all attributes except for these:
 - o `userName`
 - o `active`
 - o `name.givenName`
 - o `name.familyName`
 - o `externalId`
 - o Click Save.
5. Go back to Provisioning and under Mappings, select Provision Microsoft Entra ID Groups.
6. Under Target Object Actions, make sure Create, Update, and Delete are all selected.
7. In the attribute list, delete all attributes except for these:
 - o `displayName`
 - o `externalId`
 - o `Members`
8. Click Save.

Assign users and groups to your SCIM app integration

After configuring the provisioning settings, define which users and groups you want to sync to the Falcon platform.

Notes:

- Assigning groups: Falcon's implementation of SCIM is designed to work with groups of users. When you assign a group to your app:
 - o All group members are provisioned in Falcon.
 - o A SCIM group containing the group members is created in your CID.
 - o Any role you assign to a SCIM group in the Falcon console is inherited by its members.
 - o Entra ID does not support provisioning nested groups.
 - Assigning individuals: Provisioning users outside of group membership is not recommended. When you assign an individual user to your app:
 - o The user is automatically provisioned in Falcon with the default user settings.
 - o The user does not have a SCIM group assignment in Falcon. Belonging to a SCIM group is the only way that you can change the user's role, host group, and cloud group assignments.
1. In your Entra ID SCIM app, click Users and groups.
 2. Click + Add user/group.
 3. Under Users and groups, click None Selected.

Falcon Management

4. Click the Groups tab and select the checkbox on the groups that you want to assign to your app.
5. Click Select.
6. Click Assign.

Turn on provisioning

When configuration is complete, you can turn on provisioning to start syncing your users and groups. The initial provisioning cycle starts within 40 minutes after you turn provisioning on. After the initial cycle, changes to your users and groups are synced every 40 minutes.

Note:

- Before turning on automatic provisioning, you can select specific users and test your integration using the Provision on demand feature. For info, see [Microsoft's documentation about On-demand provisioning in Microsoft Entra ID](#).
 - Entra ID may split provisioning large numbers of users and groups into smaller batches across multiple cycles.
1. In your Entra ID SCIM app, go to Provisioning.
 2. Set Provisioning Status to On.
 3. Click Save.

Management tips and integration limitations

There are a few management tips and limitations to keep in mind for your Entra ID SCIM integration with Falcon.

Managing users and groups in Entra ID

With SCIM integration, you perform these user and group management tasks in Entra ID and the changes are reflected in Falcon.

- Adding new users to groups assigned to the SCIM app automatically adds the users to the corresponding SCIM groups in Falcon. Users inherit the roles, host groups, and cloud groups assigned to a group.
- Unassigning users from the SCIM app in Entra ID deactivates the users in Falcon.
- Removing users from groups that are assigned to the SCIM app in Entra ID removes the users from the corresponding SCIM groups in Falcon.
 - The users lose the roles and permissions granted to them through the group.
 - Users removed from all groups that are provisioned to Falcon are deactivated in Falcon and can no longer sign in.
- Unassigning a group from the SCIM app in Entra ID results in these changes in Falcon:
 - The corresponding SCIM group in Falcon is deleted.
 - Users in the group lose the roles, host groups, and cloud groups granted to them through the group.
 - If the unassigned group was a user's only provisioned SCIM group, the user is deactivated in Falcon and can no longer sign in.
- Deleting a user in Entra ID deletes the user in Falcon after 30 days.

Important note: Entra ID suspends deleted user accounts in a soft-deleted state for 30 days before permanently removing them. During that time, the user's status remains Active in the Falcon console; however, because the user is deactivated in Entra ID, they are not able to access the Falcon console using SSO through Entra ID. After 30 days, when Entra ID deletes the user, the user is also deleted from Falcon. For more info, see [Microsoft's documentation about how deprovisioning works](#).

- Updating a user's first or last names in Entra ID automatically updates the names in Falcon.
- For more info about how identity data is kept in sync with the SCIM app, see [Microsoft's documentation about provisioning cycles](#).

Managing users and groups in the Falcon console

You can view your provisioned users and SCIM groups in the Falcon console. You can also assign roles, host groups, and cloud groups to SCIM groups to manage the access permissions granted to users in those groups. For more info, see [Manage SCIM group roles, host groups, and cloud groups](#).

You cannot manage roles, host groups, and cloud groups in Entra ID.

Set up SCIM provisioning with PingOne

Use the SCIM protocol to sync user identities from PingOne to your Falcon CID. Following is a basic guide to help you set up SCIM with PingOne. For more detailed implementation info, see the [PingOne article PingOne SCIM provisioning](#).

Prerequisites

Before getting started, ensure these prerequisites are met:

Falcon Management

- Set up SSO with PingOne for your CID. For more info, see [Step 1: Set up SSO](#).
- Enable SCIM in configuration mode through the CrowdStrike Customer Center. For more info, see [Step 2: Add the SCIM feature to your Falcon CID](#).
- Get your SCIM base URL and API Key. For more info, see [Step 3: Get your SCIM base URL and API key](#).
- You must have an active PingOne subscription and administrator privileges in your account.
- Set up your user profiles and groups in PingOne.

Workflow process

The setup process includes these tasks:

1. Create a SCIM connection
2. Enable the SCIM connection
3. Configure an outbound group provisioning rule
 - a. Set the target
 - b. Define user filters
 - c. Set user attribute mappings
 - d. Select groups to provision
4. Enable the rule
5. Manage provisioned users and groups

Create a SCIM connection

Set up a SCIM connection to the Falcon platform and to your CID.

1. Log in to the PingOne Admin portal.
2. Go to Integrations > Provisioning.
3. Click + and select New connection.
4. Choose a connection type. Click Select on Identity Store.
5. Select a provisioning identity store. Choose SCIM Outbound.
6. Click Next.
7. Enter a name for the connection and an optional description.
8. Click Next.
9. Enter the following information:
 - SCIM Base URL: Enter the SCIM base URL for your CrowdStrike cloud. For the URLs, see [SCIM base URL](#).
 - SCIM Version: Select 2.0.
 - Authentication Method: Select OAuth 2 Bearer Token.
 - OAuth Access Token: Enter your CID's API key that you generated in the Falcon console as the OAuth Bearer Token value.
 - Auth Type Header: Select Bearer.
 - Users Resource: Enter /Users.
 - Group Resource: Enter /Groups.
10. Click Test Connection. This checks your base URL and API key to ensure a valid connection between Ping and your Falcon CID. If you receive an error, make sure your base URL and API key are correct and try again.
11. When Connection Successful appears, click Next.
12. In Configure Preferences, complete the following information if it's not prefilled by default.
 - User Filter Expression: Enter username Eq "%s".
 - User Identifier: Select userName.
 - Allow Users to be Created: Select the checkbox.
 - Allow Users to be Updated: Select the checkbox.
 - - Allow Users to be Disabled: Toggle on.
 - Allow Users to be Deprovisioned: Select the checkbox.
 - Remove Action: Set to Delete.
 - Deprovision on Rule Deletion: Toggle on.
13. Click Save.

Falcon Management

Enable the SCIM connection

After your connection is created, enable it from the connection details in PingOne.

1. Go to Integrations > Provisioning and click the Connections tab.
2. Click the connection in the list that you want to enable.
3. In the connection overview, click the toggle button next to the connection name to enable it.

Configure an outbound group provisioning rule

1. In PingOne, go to Integrations > Provisioning.
2. Click + and select New Rule.
3. Enter a name for the rule and an optional description.
4. Click Create Rule.

Set the target

After your rule is created, in PingOne, set your connection as the rule target.

1. In the rule configuration, click Target.

Note: If the rule configuration doesn't automatically open, go to Integrations > Provisioning and click the Rules tab. Then, click the rule in the list to open it and click the Configuration tab.

2. Under the Available Connections, click + on the connection you want to add to the rule. PingOne is populated as the Source and the added SCIM connection is set as the Target.
3. Click Save.

Define user filters

Next, define User Filter attributes in PingOne. Here, you assign your existing PingOne groups to the rule to provision the group's users. When the rule is enabled, a user account is created in your Falcon CID for each user in the assigned groups.

Note: The group itself does not sync to the Falcon platform through this step. You must add the group in the <link-to-Select-groups-to-provision-section> step to create the group in your Falcon CID.

1. In the rule configuration, click User Filter.

Note: If the rule configuration doesn't automatically open, go to Integrations > Provisioning and click the Rules tab. Then, click the rule in the list to open it and click the Configuration tab.

2. Click edit  to edit the User Filter attributes.
3. Add the following filter info for each group of users that you want to include:
 - Attribute: Select Group Names.
 - Operator: Select Contains.
 - Value: Select the group from the list of options.
4. Click Save.

Set user attribute mappings

After configuring provisioning options, set the attributes that are mapped from your SCIM app integration to the Falcon platform.

1. In the rule configuration, click Attribute Mapping.

Note: If the rule configuration doesn't automatically open, go to Integrations > Provisioning and click the Rules tab. Then, click the rule in the list to open it and click the Configuration tab.

2. Click edit  to edit the attribute mappings.
3. Keep only these attributes that are compatible to sync with Falcon. Delete all other attributes from the list.
 - Enabled (set to active)
 - Family Name (set to familyName)
 - Given Name (set to givenName)
 - Username (set to userName)

Note: You can also use Email address in place of Username. This is the PingOne field that maps to the user's email address that's used to log in to the Falcon console.

4. Click Save.

Select groups to provision

Select the PingOne groups that you want to push to Falcon. These groups are created as SCIM groups in your Falcon CID when the rule is enabled.

1. In the rule configuration, click Group Provisioning.

Falcon Management

Note: If the rule configuration doesn't automatically open, go to Integrations > Provisioning and click the Rules tab. Then, click the rule in the list to open it and click the Configuration tab.

2. Click Add Groups.
3. Select the checkbox of one or more groups to provision.
4. Click Save.
5. In the Overwrite Group Memberships window, select the acknowledgement checkbox and click Save.

Enable the rule

Turn on the rule to initiate synchronization to the Falcon platform. You can view the synced users and groups from PingOne in the Falcon console.

1. Go to Integrations > Provisioning and click the Rules tab.
2. Click the rule in the list that you want to enable.
3. In the rule overview, click the toggle button next to the rule name to enable it.

Manage provisioned users and groups

When SCIM is fully enabled, you manage your users and groups in PingOne. In the Falcon console, you can manage role, host group, and cloud group assignments for your provisioned users and groups.

Manage users and groups in PingOne

When you make these changes to your provisioned users and groups in PingOne, they're reflected in Falcon:

- Deactivating a user in PingOne deactivates the user in the Falcon console and sets the user's status to Inactive.
- Deleting a user in PingOne deletes the user in the Falcon console.
- Assigning a user to a provisioned group in PingOne automatically adds the user to the corresponding SCIM group in the Falcon console with the roles, host groups, and cloud groups allocated to the group.
- Removing a user from a provisioned group in PingOne removes them from the corresponding SCIM group in the Falcon console.
 - The user loses the roles and permissions granted to them through the group.
 - If the user is not associated with any other provisioned SCIM groups, they are deleted from the Falcon console.
- Unlinking or deleting a provisioned group in PingOne results in these actions:
 - The corresponding SCIM group is deleted in the Falcon console.
 - Users who were in the group lose the roles granted to the deleted SCIM group. Users that are not associated with any other provisioned SCIM groups are deleted from the Falcon console.
- Editing a user's first or last name in PingOne syncs to Falcon.

Manage users and groups in the Falcon console

You can view your provisioned users and SCIM groups in the Falcon console. You can also assign roles, host groups, and cloud groups to SCIM groups to manage the access permissions granted to users in those groups. For more info, see [Manage SCIM group roles, host groups, and cloud groups](#).

You cannot manage roles, host groups, and cloud groups in PingOne.

Set up SCIM provisioning with PingFederate

Use the SCIM protocol to sync user identities from your datastore to a Falcon CID using PingFederate. Following is a basic guide to help you set up SCIM with PingFederate. For more detailed implementation info, see the PingIdentity article [SCIM Provisioner](#).

Important: The Falcon console only supports SCIM 2.0. For optimal compatibility with the Falcon console, use PingFederate 12.0.

Prerequisites

Before getting started, ensure that the prerequisites outlined in this section are met.

- Your PingFederate environment must have:
 - Ping's SCIM connector installed. For more info, see the PingIdentity article [SCIM Provisioner](#).
 - A configured user datastore. For more info, see the PingIdentity article [Configuring outbound provisioning settings](#).

Note: If you're using an existing PingFederate environment, you might already have the SCIM connector installed and datastore configured.
- Set up SSO with PingFederate for your CID. For more info, see [Step 1: Set up SSO](#).
- Enable SCIM in configuration mode through the CrowdStrike Customer Center. For more info, see [Step 2: Add the SCIM feature to your Falcon CID](#).
- Get your SCIM base URL and API Key. For more info, see [Step 3: Get your SCIM base URL and API key](#).
- You must have an active PingFederate subscription and administrator privileges in your account.
- Set up your user profiles and groups in PingFederate.

Falcon Management

Workflow process

The setup process includes these tasks:

1. Create a SCIM connection
2. Configure a provisioning channel
3. Enable the SCIM connection
4. Manage users and groups

Create a SCIM connection

Set up a SCIM provisioning connection to the Falcon console and to your CID. For more detailed setup info, see the PingIdentity article [Creating a provisioning connection](#).

Note for Falcon Flight Control accounts:

If you want to provision users in multiple CIDs, then you must create a new SCIM connection for each CID in which there are users to be provisioned.

1. Log in to the PingFederate administrative console.
2. Go to Integration > SP Connections.
3. Click Create Connection.
4. On the Connection Template tab, select Use a template for this connection. Choose SCIM Connector.
5. Click Next.
6. On the Connection Type tab, ensure that the Outbound provisioning box is checked.
7. Click Next.
8. On the General Info tab, enter a name for the connection and other details.
9. Click Next.
10. On the Outbound Provisioning tab, click Configure Provisioning.
11. On the Target tab, configure your SCIM target settings. For more info about these settings, see the PingIdentity article [SCIM provisioner settings reference](#).
 - SCIM URL: Enter the SCIM base URL for your CrowdStrike cloud. For the URLs, see [SCIM base URL](#).
 - SCIM Version: Select 2.0.
 - Authentication Method: Select OAuth 2 Bearer Token.
 - Access Token: Enter your CID's API key that you generated in the Falcon console as the OAuth Bearer Token value.
 - Authorization Header Type: Enter Bearer.
 - Users API Path: Enter /Users.
 - Groups API Path: Enter /Groups.
 - Results Per Page: We recommend 250.
 - Provisioning Options: We recommend selecting User Create, User Update, and User Disable/Delete. Optionally, select Provision Disabled Users.
 - Remove User Action: Configure as per your preference.
 - Group Name Source: We recommend selecting Use Patch for Group Updates.
12. Click Next.

Configure a provisioning channel

Configure the provisioning channel where user details will be sourced from.

1. On the Manage Channels tab, click Create.
2. On the Channel Info tab, enter the channel details. For more info, see the PingIdentity article [Specifying channel information](#).
3. Click Next.
4. On the Source tab, select your Active data store. For more info, see the PingIdentity article [Identifying the source datastore](#).
5. Click Next.
6. The details found on the Source Settings, Source Location, and Attribute Mapping tabs are determined as per your datastore provider.
7. On the Source Settings tab, specify your source settings. For more info, see the PingIdentity article [Modifying source settings](#).
8. Click Next.
9. On the Source Location tab, specify the attributes based on your datastore provider to determine which users and groups should be provisioned to the Falcon console. For more info, see the PingIdentity article [Specifying a source location](#).
10. Click Next.
11. On the Attribute Mapping tab, set your user attribute mappings. Enter Attribute(s) for these Field Names, which are required by the Falcon console:
 - userName: The user's email address. For existing Falcon console users, make sure this email matches the user's email address in the Falcon console.
 - familyName: The user's last name.
 - givenName: The user's first name.
 - For more info, see the PingIdentity article [Mapping attributes](#).
12. Click Next.
13. On the Activation & Summary tab, for the Channel Status, select Active.
14. Click Done.
15. On the Configure Channels page, click Done.

Enable the SCIM connection

After your connection is set up, enable it from the activation details in PingFederate.

1. On the SP Connections page, go to the Activation & Summary tab.
2. Verify that the details are correct and click Save.
3. On the SP Connections page that opens, ensure that your connection is Enabled.

When your connection is enabled, users and groups from your source repository will start provisioning to the Falcon console.

Falcon Management

Manage users and groups

When SCIM is fully enabled in PingFederate, you manage your users and groups in your provisioning source repository. In the Falcon console, you can manage role, host group, and cloud group assignments for your provisioned users and groups.

Manage users and groups in your provisioning source repository

When you make these changes to your provisioned users and groups in your provisioning source repository, they're reflected in the Falcon console:

- Deactivating a user in your provisioning source repository deactivates the user in the Falcon console and sets the user's status to Inactive.
- Deleting a user in your provisioning source repository deletes the user in the Falcon console.
- Assigning a user to a provisioned group in your datastore prompts your provisioning source repository to automatically add the user to the corresponding SCIM group in the Falcon console with the roles, host groups, and cloud groups allocated to the group.
- Removing a user from a provisioned group in your provisioning source repository removes them from the corresponding SCIM group in the Falcon console.
 - The user loses the roles and permissions granted to them through the group.
 - If you remove a user from a provisioned group and they are also removed from the Source Location selector, the user is then either disabled or deleted from the Falcon console depending on how you have configured your target settings on the Target tab.
- Unlinking or deleting a provisioned group in your provisioning source repository results in these actions:
 - The corresponding SCIM group is deleted in the Falcon console.
 - Users who were in the group lose the roles granted to the deleted SCIM group.
 - If you remove a provisioned group and the members of the group are also removed from the Source Location selector, those users are then either disabled or deleted from the Falcon console depending on how you have configured your target settings on the Target tab.
- Editing a user's first or last name in your provisioning source repository syncs to the Falcon console.

Manage users and groups in the Falcon console

You can view your provisioned users and SCIM groups in the Falcon console. You can also assign roles, host groups, and cloud groups to SCIM groups to manage the access permissions granted to users in those groups. For more info, see [Manage SCIM group roles, host groups, and cloud groups](#).

You cannot manage roles, host groups, and cloud groups in PingFederate.

Single Sign-On (SSO) for Falcon

Set up Falcon console to use single sign-on (SSO) authentication for simplified user management and improved security controls.

Introduction

This guide describes how to set up your organization's Falcon console to use single sign-on (SSO) for authentication. This simplifies user management and improves security controls.

If you set up SSO, it replaces Falcon's standard sign-in process. You can temporarily use an onboarding mode while you transition between existing Falcon authentication and SSO. After you've fully transitioned to SSO, your authentication mode is referred to as full SSO.

Before you begin

Supported identity providers

In general, customers have configured Falcon authentication using many SAML 2.0 identity providers.

Note: Falcon's SAML metadata is updated daily with today's date.

CrowdStrike has specifically tested and confirmed these IdPs:

- Active Directory Federation Services (AD FS)
- Okta
- PingFederate
 - Versions 8.2 - 8.4
 - Versions 9.1 and later
- PingOne
- Microsoft Entra ID

Note: For info about supported web browsers, see [Supported browsers](#).

Using SSO and Just-in-Time Provisioning

If Just-in-Time provisioning is not configured, Falcon's SSO integration applies only to authentication. In other words, we support identity assertion, including signed and encrypted assertions. This integration doesn't support more complex SSO functionality, such as automatic user account provisioning and deprovisioning, user group management or sync, or single logout.

If Just-in-Time provisioning is configured, Falcon's SSO integration supports automatic user account provisioning, role management, and user group management. During account provisioning, the user must initially log in to the Falcon console using the IdP-initiated login link. User account deprovisioning must be done manually.

Important: System for Cross-domain Identity Management (SCIM) is not supported with Just-in-Time provisioning.

User account management

You can create user accounts manually or automatically, as discussed in these sections:

Falcon Management

- [Manual user account management](#)
- [Automated user account setup with Just-in-Time provisioning](#)

Manual user account management

This section covers creating user accounts manually. For info about automating the provisioning of user accounts, see [Automated user account setup with Just-in-Time provisioning](#).

- **Creating users:**
 - **Onboarding mode:** Newly created user accounts are inactive. Users must activate the account using a link emailed to them.
 - **Full SSO:** All new users are immediately active.
- **Removing users:** To remove inactive users, delete the users in the Falcon console.
- **Roles:** Manage Falcon's user roles in Falcon, not in your IdP.
- **Passwords and 2FA:** If SSO is already enabled in your environment, reset passwords or configure two-factor authentication (2FA) settings in your IdP, not in Falcon.

Automated user account setup with Just-in-Time provisioning

Just-in-Time (JIT) provisioning automates the creation of Falcon user accounts by delegating the task to the identity provider (IdP). For info about creating user accounts manually, see [Manual user account management](#).

- **Creating users:** If you complete the Just-in-Time steps for configuring your IdP, users who log in to the Falcon console using the IdP-initiated login link get Falcon accounts created automatically.
- **Removing users:** To remove inactive users, delete the users in the Falcon console.

As part of your IdP configuration, you can set SAML attributes to specify various settings for users. Here are the relevant attributes:

- `firstName`
- `lastName`
- `roles`

Specifies CrowdStrike role IDs for the user. By default, the ID value is `falcon_console_guest`.

Important: The corresponding roles in Falcon must already exist. Create any new roles in Falcon before configuring your IdP to use the new roles. If you specify a role that doesn't exist in Falcon—or is not allowed for the user, the Falcon login is attempted with any other roles you specified. If no valid roles are specified, the login fails. The default is not used.

Important: Each time a user logs in to the Falcon console, the user's roles are determined by this attribute. This attribute's value overrides any changes made to a user's roles in the Falcon console. If this value is not set, any changes you make in the console are left unchanged. Manage the user's roles using either your IdP configuration or through the Falcon console—but not both.

- `userGroups`

For Falcon Flight Control environments: Specifies the IDs for the user groups in the parent CID to include the user in. Also removes the user from any other user groups upon login. This attribute has no default value.

Important: The corresponding user groups in Falcon must already exist. Create any new user groups in Falcon before configuring your IdP to use the new user groups.

Important: Each time a user logs in to the Falcon console, the user's groups are determined by this attribute. This attribute's value overrides any changes made to a user's groups in the Falcon console. If this value is not set, any changes you make in the console are left unchanged. Manage the user's groups using either your IdP configuration or through the Falcon console—but not both.

- `homeCID`

For Falcon Flight Control environments: If you use the same SAML configuration—with the same issuer or entity ID—across all of your CIDs, use this attribute to specify the user's home CID.

For info about how to set these attributes for the various IdPs, see [Step 1: Configure your IdP](#).

Falcon Flight Control support

With Just-in-Time provisioning, if you use Falcon Flight Control, be aware of the following facts:

- You can only set a user's roles in the user's home CID. Use the Falcon console to give a user roles in other CIDs.
- You can assign users in parent CIDs to any number of user groups by using the `userGroups` SAML attribute in your IdP configuration.
- To give users whose home CID is the parent CID direct grant roles, use the SAML assertion with the `roles` attribute. To give these users membership in parent user groups, use the SAML assertion with the `userGroups` attribute.

Enabling Just-in-Time provisioning

For info about how to enable Just-in-Time provisioning, see [Step 2: Contact us to configure Falcon SSO for your organization](#).

Disabling Just-in-Time provisioning

To disable Just-in-Time provisioning, contact Support using the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, contact [CrowdStrike Government Customer Center](#).

Any users who were provisioned in the Falcon console when Just-in-Time provisioning was enabled will still be able to log in even after Just-in-Time provisioning is disabled.

Single sign-on terminology

You should be familiar with some common, industry-standard terms related to single sign-on.

Falcon Management

- Single sign-on (SSO): A single authentication system that can be used to access multiple software systems. You can set up an SSO solution to simplify login processes for your users and to centralize user management for your administrators.
- Service Provider (SP): The specific application you want to access using SSO. For this guide, the SP is the Falcon console. Other resources sometimes use the name "relying party (RP)".
- Identity Provider (IdP): The service that handles your SSO authentication and manages your users' identity information. For this guide, the IdP is your SSO solution, such as Okta, Ping, or AD FS.
- Security Assertion Markup Language (SAML): A protocol used to implement SSO. Falcon supports SAML 2.0, a widely used standard that's supported by many IdPs.
- Application: A set of configuration options that tells your IdP how to interact with Falcon and that governs which of your IdP users can use SSO to access Falcon.

Certificate requirements

As defined in RFC 5280, SAML certificates must have positive serial numbers. Certificates with negative serial numbers are not supported.

Set up and use SSO

This list gives you an overview of the tasks you must complete to set up and use SSO. For details, see the linked sections.

If you're already using SSO but want to enable Just-in-Time provisioning, see [Update your SSO configuration to use Just-in-Time provisioning](#).

Step 1: Configure your IdP

- Active Directory Federation Services (AD FS)
- Okta
- PingFederate
- PingOne
- Microsoft Entra ID

Step 2: Contact us to configure Falcon SSO for your organization

Step 3: Test logging in with SSO

Step 4: Transition to SSO authentication

Step 1: Configure your IdP

The process to create and assign a new application follows this general pattern. After the general pattern, you can find IdP-specific instructions.

1. Access your IdP's application settings.
2. Add a new application to your IdP.
 - Provide Falcon's SP URL for the CrowdStrike cloud you're using. Check the domain for your Falcon console and use the following SP URL with the matching domain:
 - US-1: <https://falcon.crowdstrike.com/saml/acs>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/acs>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/acs>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/acs>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/acs>
 - Provide Falcon's SAML metadata for the CrowdStrike cloud you're using. Check the domain for your Falcon console and use the following SAML metadata with the matching domain:
 - US-1: <https://falcon.crowdstrike.com/saml/metadata>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/metadata>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/metadata>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/metadata>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/metadata>
 - Map your user's IdP username to their Falcon email address.
 - You might need to create a mapping to specify Falcon role IDs.

To get the ID for a role, you have these options:

 - Use an API endpoint

The endpoint to use is: `GET /user-management/queries/roles/v1`

For more info, see [Users and Roles APIs](#).
 - Use the Falcon console

Go to [Host setup and management](#) > [Falcon users](#) > [Roles and permissions](#). Find the role you want the ID for. Click  for that role and select [View role details](#). Look at your browser's address bar. The ID is in the URL, `.../roles-and-permissions/<role_ID>/permissions`, shown by the `<role_ID>` value.
3. Assign your IdP application to your IdP users.

For info about configuring a specific IdP application, see the section for your application:

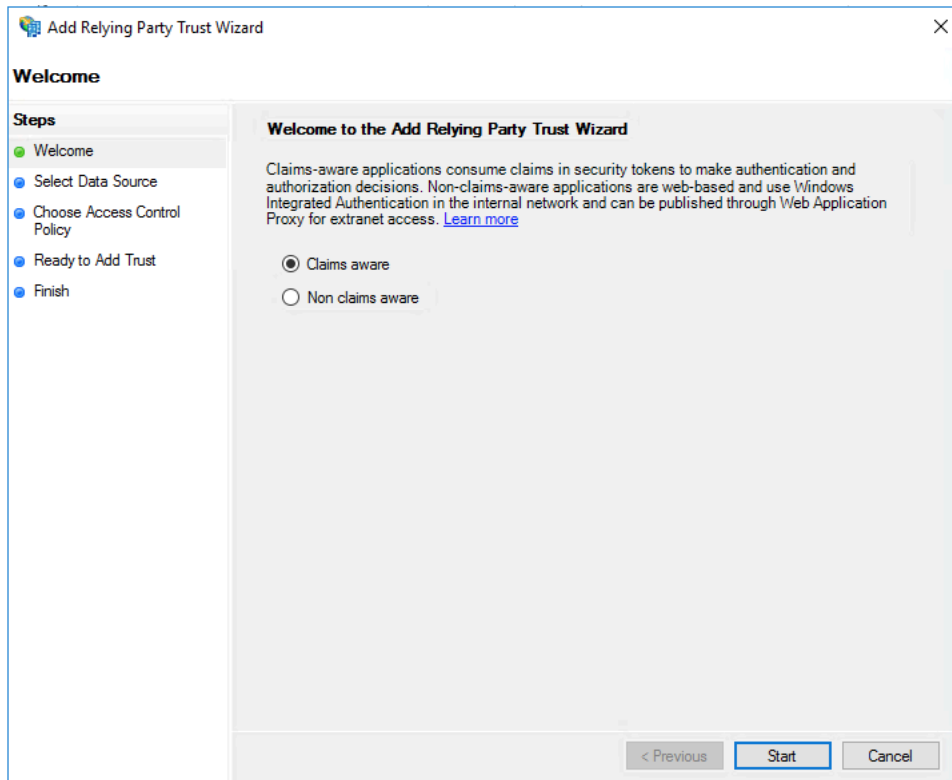
Falcon Management

- Active Directory Federation Services (AD FS)
- Okta
- PingFederate
- PingOne
- Microsoft Entra ID

Active Directory Federation Services (AD FS)

Note: These steps and screenshots shown were taken from AD FS version 4.0 on Windows Server 2016. Similar steps apply to other versions of AD FS or Windows Server. For more information, see [Microsoft's documentation](#).

1. Create a new relying party trust.
 - a. Open your AD FS Management Console.
 - b. Add a new relying party trust.
 - c. Select Claims aware.



- d. Click Start.
- e. In the Federation metadata address field, enter CrowdStrike's metadata URL for the CrowdStrike cloud you're using. Check the domain for your Falcon console and use the following metadata URL with the matching domain:
 - US-1: `https://falcon.crowdstrike.com/saml/metadata`
 - US-2: `https://falcon.us-2.crowdstrike.com/saml/metadata`
 - EU-1: `https://falcon.eu-1.crowdstrike.com/saml/metadata`
 - US-GOV-1: `https://falcon.laggar.gcw.crowdstrike.com/saml/metadata`
 - US-GOV-2: `https://falcon.us-gov-2.crowdstrike.mil/saml/metadata`

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar says 'Add Relying Party Trust Wizard' with a close button. The main heading is 'Select Data Source'. On the left, there's a 'Steps' pane with five items: 'Welcome' (selected), 'Select Data Source', 'Choose Access Control Policy', 'Ready to Add Trust', and 'Finish'. The main area contains three radio button options for selecting a data source. The first option, 'Import data about the relying party published online or on a local network', is selected. Below it, a text box contains the URL 'https://falcon.crowdstrike.com/saml/metadata'. The second option is 'Import data about the relying party from a file', and the third is 'Enter data about the relying party manually'. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☒ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

☐ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

Note: If your ADFS server can't access our metadata URL, download the metadata XML file directly from the URL using Google Chrome's More Tools > Save Page As. Then use this wizard's Import data about the relying party from a file option.

f. Click Next.

g. Set your trust's name and permissions as required for your AD FS environment.

2. Configure the AD FS claims for your relying party trust to map your users' email addresses to the Name ID field of the SAML response. To do so, create two rules: one for sending claims and one for receiving claims.

a. Select your relying party trust, and choose Edit Claim Issuance Policy.

b. Create a rule for sending claims. The specific LDAP attribute varies depending on your AD configuration.

i. Click Add Rule.

ii. For the Claim rule template, choose Send LDAP Attribute as Claims.

iii. Enter any Claim rule name as a descriptive label.

iv. For the Attribute store, choose Active Directory.

v. Add one row mapping the LDAP attribute that contains users' email addresses, such as User-Principal-Name, to the outgoing claim type E-Mail Address.

Note: This example should work in most cases. If not, use E-Mail Address for both LDAP attribute and outgoing claim type.

Edit Rule - Email ✕

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	E-Mail Address
*		

c. Create a second rule for receiving claims.

i. Click Add Rule.

ii. For the Claim rule template, choose Transform an Incoming Claim.

iii. Set the following attributes for transforming incoming claims:

- Incoming claim type: E-Mail Address
- Outgoing claim type: Name ID
- Outgoing name ID format: Email

iv. Leave Pass through all claim values selected

Edit Rule - Name ID ✕

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

3. Click OK.

Falcon Management

4. Optional. Create a rule to support Just-in-Time provisioning. For more info about this provisioning and the following attributes, see [Automated user account setup with Just-in-Time provisioning](#).

a. Click Add Rule.

b. For first name, last name, and home CID, set the attributes as follows:

i. For the Claim rule template, select Send LDAP Attributes as Claims.

ii. Set the case-sensitive attributes as follows:

- firstName: Required. Map the LDAP attribute to Given Name.
- lastName: Required. Map the LDAP attribute to Surname.
- homeCID: Optional. For CrowdStrike Flight Control environments. Name of the CID.

If you manage all your users with one IdP, it's best to use a mapping of the IdP-based user groups, such as AD groups, for the CID instead of a static CID assignment.

c. For the user roles and the Flight Control user groups, set the attributes as follows:

i. For the Claim rule template, select Send Group Membership as a Claim.

ii. Set the case-sensitive attributes as follows:

- For the claim rule name: roles

Optional. Use a mapping of the IdP-based user groups, such as AD groups, to specify the role IDs, comma-separated.

To get the ID for a role, you have these options:

- Use an API endpoint

The endpoint to use is: GET /user-management/queries/roles/v1

For more info, see [Users and Roles APIs](#).

- Use the Falcon console

Go to [Host setup and management > Falcon users > Roles and permissions](#). Find the role you want the ID for. Click  for that role and select View role details. Look at your browser's address bar. The ID is in the URL, .../roles-and-permissions/<role_ID>/permissions, shown by the <role_ID> value.

- For the claim rule name: userGroups

Optional. For CrowdStrike Flight Control environments.

Use a mapping of the IdP-based user groups, such as AD groups, to specify the user group IDs, comma-separated.

To get the ID for a Flight Control user group, you have these options:

- Use an API endpoint

For more info, see <https://assets.falcon.crowdstrike.com/support/api/swagger.html#/mssp/queryUserGroups>.

- Use the Falcon console

Using the parent CID, go to [Host setup and management > Flight Control management > User groups](#). Find the user group you want the ID for. Click  for that group and select View user group. Look at your browser's address bar. The ID is in the URL, .../roles-and-user-groups/<group_ID>/users, shown by the <group_ID> value.

5. Click OK.

Retrieving AD FS metadata

AD FS makes its metadata XML file available at a URL that varies depending on your AD FS configuration (default: <https://<host>:<port>/Federation/Metadata/2007-06/FederationMetadata.xml>).

Falcon only accepts metadata encoded as UTF-8.

Okta

For more information about configuring Okta, see [Okta's documentation](#).

1. Sign in to your Okta developer account.

Note: You must have administrative privileges to create an app integration.

2. Create an app integration for Falcon.

a. From the Admin Console, go to Applications > Applications.

b. Click Create App Integration.

c. For Sign-in method, select SAML 2.0.

d. Click Next.

e. Add required values to your application's configuration:

Falcon Management

- App name: a descriptive label, such as "CrowdStrike Falcon"
- Single sign on URL: Check the domain for your Falcon console and use the following URL with the matching domain:
 - US-1: <https://falcon.crowdstrike.com/saml/acs>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/acs>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/acs>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/acs>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/acs>
- Audience URI (SP Entity ID): Check the domain for your Falcon console and use the following URL with the matching domain:
 - US-1: <https://falcon.crowdstrike.com/saml/metadata>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/metadata>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/metadata>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/metadata>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/metadata>
- Name ID format: EmailAddress
- Application username: Email

3. Optional. Create attribute statements to support Just-in-Time provisioning. For more info about this provisioning and the following attributes, see [Automated user account setup with Just-in-Time provisioning](#).

- a. Go to Applications.
- b. Select your application for Falcon.
- c. Click the General tab.
- d. Scroll to the SAML settings.
- e. Click Edit.
- f. Click Next.

You should see the SAML settings now.

g. Scroll to Attribute Statements.

h. Required. For first name and last name, set the name formats as follows:

- For first name:
 - Attribute name: `firstName`
 - Name format: `Basic`
 - Value: `user.firstName`
- For the last name:
 - Attribute name: `lastName`
 - Name format: `Basic`
 - Value: `user.lastName`

i. Optional. For CrowdStrike Flight Control environments.

For the home CID, set the name format as follows:

- Attribute name: `homeCID`
- Name format: `Basic`
- Value: The name of the CID

If you manage all your users with one IdP, it's best to use a mapping of the IdP-based user groups, such as AD groups, for the CID instead of a static CID assignment.

j. For the user roles and the CrowdStrike Flight Control user groups, the name format is unspecified. Set the attributes as follows.

Falcon Management

- Optional. For the roles:

- Attribute name: roles
- Name format: Unspecified
- Value: Use the Okta expression language to map Okta groups to Falcon role IDs, comma-separated.

For more info about this language, see the Okta article [Okta Expression Language overview](#)

To get the ID for a role, you have these options:

- Use an API endpoint

The endpoint to use is: GET /user-management/queries/roles/v1

For more info, see [Users and Roles APIs](#).

- Use the Falcon console

Go to [Host setup and management](#) > [Falcon users](#) > [Roles and permissions](#) . Find the role you want the ID for. Click  for that role and select [View role details](#). Look at your browser's address bar. The ID is in the URL, .../roles-and-permissions/<role_ID>/permissions, shown by the <role_ID> value.

Example:

```
isMemberOfGroupName("Admins") ? "falconhost_admin,intel_admin" :  
isMemberOfGroupName("Analysts") ? "falconhost_analyst,intel_basic_analyst" : null
```

- Optional. For CrowdStrike Flight Control environments.

For the Flight Control user groups:

- Attribute name: userGroups
- Name format: Unspecified
- Value: Use the Okta expression language to map Okta groups to Flight Control user groups by ID, comma-separated. For more info about this language, see the Okta article [Okta Expression Language overview](#)

To get the ID for a Flight Control user group, you have these options:

- Use an API endpoint

For more info, see <https://assets.falcon.crowdstrike.com/support/api/swagger.html#/mssp/queryUserGroups>.

- Use the Falcon console

Using the parent CID, go to [Host setup and management](#) > [Flight Control management](#) > [User groups](#) . Find the user group you want the ID for. Click  for that group and select [View user group](#). Look at your browser's address bar. The ID is in the URL, .../roles-and-user-groups/<group_ID>/users, shown by the <group_ID> value.

Example:

```
isMemberOfGroupName("Admins") ?  
"535b7eb1af2f4fc89b665184bca26201,7d59468ff16443e1b70777882aca93f0" :  
isMemberOfGroupName("Analysts") ? "808d754027e1472a8adace3ec284edf2" : null
```

- k. Proceed to the end of the form and click [Finish](#).

4. Assign your application to your users.

- Go to [Applications](#) > [Applications](#).
- Click [Assign Users to App](#).
- Assign your Falcon application to any users you choose.

Note: When you're first setting up SSO, assign access only to a test user group. You can return later to assign more users throughout your organization.

- Click [Next](#).
- Confirm your users' email addresses.
- Click [Confirm Assignments](#).

PingFederate

Note: These steps and screenshots shown were taken from PingFederate versions 9.1.3 and 8.2.0. Similar steps apply to other supported versions of PingFederate. For more info, see [Ping's documentation](#).

Configure your PingFederate environment to use these settings.

1. Assertion creation

- Go to [SP Connection](#) > [Browser SSO](#) > [Assertion Creation](#).
- Under [Identity Mapping](#), set the attribute contract item SAML_SUBJECT to emailAddress.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping	Attribute Contract	Authentication Source Mapping	Summary
------------------	--------------------	-------------------------------	---------

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract	Subject Name Format
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Extend the Contract	Attribute Name Format
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic

3. Optional. Create a rule to support Just-in-Time provisioning. For more info about this provisioning and the following attributes, see [Automated user account setup with Just-in-Time provisioning](#).

- Click Add Rule.
- Create an Attribute Contract for the attributes.
- For first name, last name, and home CID, set the attributes as follows:

- Set the case-sensitive attribute formats as follows:

- firstName: Required. Basic
- lastName: Required. Basic
- homeCID: Optional. For CrowdStrike Flight Control environments. Unspecified

- Click Next.

That takes you to the Attribute Mapping tab.

- Add mappings to set the values of the new attributes as follows:

- firstName: Given Name
- lastName: Surname
- homeCID: Enter the string

If you manage all your users with one IdP, it's best to use a mapping of the IdP-based user groups, such as AD groups, for the CID instead of a static CID assignment.

- Create an Attribute Contract for these attributes

- For the user roles and the Flight Control user groups, set the attribute formats as follows:

- roles: Optional. Unspecified
- userGroups: Optional. For CrowdStrike Flight Control environments. Unspecified

- Click Next.

That takes you to the Attribute Mapping tab.

- Add mappings to set the values of the new attributes as follows:

Note: For attribute mapping with the Object Graph Navigation Language (OGNL): Starting with PingFederate version 10.1, expressions are enabled by default. Before version 10.1, you must enable expressions as explained in the Ping Identity article [Enabling and disabling expressions](#). For info about OGNL, see the Ping Identity article [Construct OGNL expressions](#).

- roles: Use OGNL to map current user roles to role IDs.

Use a mapping of the IdP-based user groups, such as AD groups, to specify the role IDs, comma-separated.

To get the ID for a role, you have these options:

- Use an API endpoint

The endpoint to use is: GET /user-management/queries/roles/v1

For more info, see [Users and Roles APIs](#).

- Use the Falcon console

Go to [Host setup and management](#) > [Falcon users](#) > [Roles and permissions](#). Find the role you want the ID for. Click  for that role and select [View role details](#). Look at your browser's address bar. The ID is in the URL, .../roles-and-permissions/<role_ID>/permissions, shown by the <role_ID> value.

- userGroups: Use OGNL to map current user groups to user groups IDs.

Use a mapping of the IdP-based user groups, such as AD groups, to specify the user group IDs, comma-separated.

To get the ID for a Flight Control user group, you have these options:

Falcon Management

- Use an API endpoint

For more info, see <https://assets.falcon.crowdstrike.com/support/api/swagger.html#mssp/queryUserGroups>.

- Use the Falcon console

Using the parent CID, go to **Host setup and management > Flight Control management > User groups**. Find the user group you want the ID for. Click  for that group and select **View user group**. Look at your browser's address bar. The ID is in the URL, `.../roles-and-user-groups/<group_ID>/users`, shown by the `<group_ID>` value.

e. Save your changes.

2. IdP adapter mapping

1. Go to **SP Connection > Browser SSO > Assertion Creation > IdP Adapter Mapping**.
2. Configure an adapter instance that corresponds to your organization's user management setup.
 - The attribute contract item `SAML_SUBJECT` must be mapped to the user's email address as it appears in Falcon.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance	Mapping Method	Attribute Contract Fulfillment	Issuance Criteria	Summary
------------------	----------------	--------------------------------	-------------------	---------

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
SAML_SUBJECT	Adapter 	username 	None available

3. Protocol settings

1. Go to **SP Connection > Browser SSO > Protocol Settings**.
2. Under **Allowable SAML Bindings**, Choose **Post** and/or **Redirect**. **Artifact** or **SOAP** are unsupported.
3. Under **Signature Policy**:
 - Deselect **Require Authn Requests to be signed...**
 - Select **Always sign assertion** if your PingFederate environment uses encrypted assertions.
 - Select **Sign response as required**. (This option is not available for PingFederate versions 8.2 - 8.4.)

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL	Allowable SAML Bindings	Signature Policy	Encryption Policy	Summary
--------------------------------	-------------------------	------------------	-------------------	---------

Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to require choose to sign assertions sent to this partner, regardless of the binding used.

☐	REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS
☒	ALWAYS SIGN ASSERTION
☒	SIGN RESPONSE AS REQUIRED

4. Under **Encryption Policy**:
 - If you selected **Always sign assertion** under **Signature Policy**, select **The entire assertion here**.
 - If you deselected **Always sign assertion** under **Signature Policy**, select **None here**.

4. SP Connection > Credentials

1. Go to **SP Connection > Credentials**.
2. Specify all required credentials. The options available on this page vary slightly depending on the configuration choices you've made earlier.
 - For **Signing Certificate**, we recommend selecting **Include the certificate in the signature element**.
 - We don't recommend selecting **Include the raw key...**, as there is no additional benefit.

3. Select any signing algorithm. If you're not sure which to select, we recommend SHA-512.

SP Connection | Credentials

Digital Signature Settings

Summary

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE

01:66:8E:9F:76:CF (CN=ssotest-pingfed913.devtest.eyrie...) ▼



INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.



INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM

RSA SHA256 ▼

Manage Certificates

PingOne

For more information about configuring PingOne, see the [Ping documentation](#).

1. Log in to PingOne.
2. Create an application for Falcon.
 - a. Go to Applications.
 - b. Click Add Application.

My Applications

Applications you've added to your account are listed here. You can search by application name, description or entityId

- *Active* applications are enabled for single sign-on (SSO).
- *Details* displays the application details.

Application Name	Type	Status	Enabled	
[Application Name]	SAML	Active	Yes	Remove
[Application Name]	SAML	Active	Yes	Remove

Add Application

- Search Application Catalog
- New SAML Application**
- Request Ping Identity add a new application to the application catalog

Pause All SSO

- c. Select New SAML Application.
- d. Enter a descriptive label for the required fields:
 - Application Name
 - Application Description
 - Category
- e. Click Continue to Next Step.

Falcon Management

f. Near the top, select I have the SSO URL.

2. Application Configuration

I have the SAML configuration

I have the SSO URL

Tell us the SSO URL to use for your application. This URL will be used by PingOne.

SSO URL

https://falcon.crowdstrike.com/saml/acs

NEXT: Review Setup

Cancel

Back

Save & Exit

Save & Publish

g. For the SSO URL, check the domain for your Falcon console and use the following URL with the matching domain:

- US-1: <https://falcon.crowdstrike.com/saml/acs>
- US-2: <https://falcon.us-2.crowdstrike.com/saml/acs>
- EU-1: <https://falcon.eu-1.crowdstrike.com/saml/acs>
- US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/acs>
- US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/acs>

h. Click Save & Publish.

i. Assign your application to your users.

j. Go to Users.

k. Click User Groups.

l. Near the group you want to assign access to your application, click Edit.

Note: When you're first setting up SSO, assign access only to a test user group. You can return later to assign more users throughout your organization.

m. Select your application for Falcon.

n. Click Save.

o. Optional. Create an attribute mapping to support Just-in-Time provisioning. For more info about this provisioning and the following attributes, see [Automated user account setup with Just-in-Time provisioning](#).

- Go to My Applications.
- Select your application for Falcon.
- Select Attribute Mappings.
- Select Edit.

v. Required. For first name and last name, under the Attributes column, set the case-sensitive attribute names as follows:

- firstName: Map to Given Name
- lastName: Map to Family Name

vi. Optional. For CrowdStrike Flight Control environments.

For the home CID, set the case-sensitive attribute as follows:

homeCID: Select Advanced Expression and enter the name of the CID as a quoted string: "my CID"

If you manage all your users with one IdP, it's best to use a mapping of the IdP-based user groups, such as AD groups, for the CID instead of a static CID assignment.

vii. Click Save.

viii. Optional. For the user roles and the Flight Control user groups, set the attributes as follows:

- Select Advanced Expression and using the PingOne expression language, specify the mapping of PingOne groups to Falcon user role IDs, comma-separated. For info about this language, see the Ping Identity article [PingOne expression language](#).

To get the ID for a role, you have these options:

- Use an API endpoint

The endpoint to use is: `GET /user-management/queries/roles/v1`

For more info, see [Users and Roles APIs](#).

- Use the Falcon console

Go to [Host setup and management > Falcon users > Roles and permissions](#). Find the role you want the ID for. Click  for that role and select View role details. Look at your browser's address bar. The ID is in the URL, `.../roles-and-permissions/<role_ID>/permissions`, shown by the `<role_ID>` value.

As an example, consider this expression:

```
#core.ifElse(#data.containsAny(user.memberOfGroupNames, "Admins"), "falconhost_admin,intel_admin",
#data.containsAny(user.memberOfGroupNames, "Analysts"), "falcon_analyst,intel_basic_analyst",
```

Falcon Management

```
#data.containsAny(user.memberOfGroupNames, "Everyone"), "falcon_analyst")
```

The results of this expression are as follows:

If you're in the Admins group, you get the Falcon Admin and Intel Admin user roles.

If you're in the Analysts group, you get the Falcon Analyst and Intel Admin user roles.

If you're in the Everyone group, you get the Falcon Analyst user role.

2. For mappings of PingOne groups to Falcon Flight Control user groups, use the expression language to map to user group IDs, comma-separated.

To get the ID for a Flight Control user group, you have these options:

- Use an API endpoint

For more info, see <https://assets.falcon.crowdstrike.com/support/api/swagger.html#/mssp/queryUserGroups>.

- Use the Falcon console

Using the parent CID, go to **Host setup and management > Flight Control management > User groups**. Find the user group you want the ID for. Click  for that group and select **View user group**. Look at your browser's address bar. The ID is in the URL, `.../roles-and-user-groups/<group_ID>/users`, shown by the `<group_ID>` value.

- ix. Save your changes.

Microsoft Entra ID

For more information about configuring Entra ID, see [Microsoft's documentation](#).

1. In the Microsoft Entra console, go to Entra ID.
2. Find the Manage section and select single sign-on.
3. On the Select a single sign-on method page, select SAML.
4. Click to edit the Basic SAML Configuration settings.
5. In the Basic SAML Configuration section, enter the values for the following fields:

- a. Enter the Reply URL (Falcon's SP URL).

Check the domain for your Falcon console and use the following URL with the matching domain.

Select the box for the ACS URL for your CID.

- US-1: <https://falcon.crowdstrike.com/saml/acs>
- US-2: <https://falcon.us-2.crowdstrike.com/saml/acs>
- EU-1: <https://falcon.eu-1.crowdstrike.com/saml/acs>
- US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/acs>
- US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/acs>

- b. Enter the Identifier (Falcon's SAML metadata).

Select the cloud Entity URL that corresponds to the cloud your CID uses.

Remove the identifiers that aren't associated with your CID.

- US-1: <https://falcon.crowdstrike.com/saml/metadata>
- US-2: <https://falcon.us-2.crowdstrike.com/saml/metadata>
- EU-1: <https://falcon.eu-1.crowdstrike.com/saml/metadata>
- US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/metadata>
- US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/metadata>

- c. If you're using SP-initiated logins, enter the Sign on URL.

Note: For IdP-initiated logins, leave this field blank. If you're using SP-initiated logins in trial mode, remove the URL in this field when you switch to full SSO to allow for IdP-initiated logins.

- US-1: <https://falcon.crowdstrike.com/login/sso>
- US-2: <https://falcon.us-2.crowdstrike.com/login/sso>
- EU-1: <https://falcon.eu-1.crowdstrike.com/login/sso>
- US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/login/sso>
- US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/login/sso>

6. Copy the app federation metadata URL.

- a. In the left navigation, click Single sign-on.

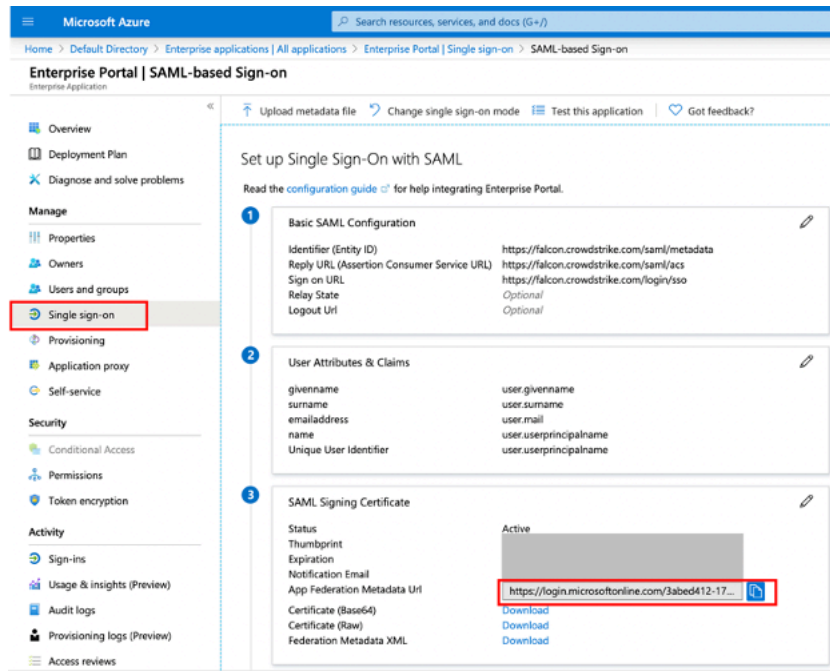
- b. If needed, configure or reconfigure the URLs.

- c. Copy the URL in the App Federation Metadata Url field. Make sure the URL contains `?appid=<APP ID>`. For example:

<https://login.microsoftonline.com/<TENANT ID>/federationmetadata/2007-06/federationmetadata.xml?appid=<APP ID>>

Falcon Management

Keep this URL to provide to CrowdStrike support.



7. Optional. Add claims to support Just-in-Time provisioning. For more info about this provisioning and the following attributes, see [Automated user account setup with Just-in-Time provisioning](#).

a. For first name, last name, and home CID, set the attributes as follows:

i. In your single sign-on application SAML setup, select to edit User Attributes & Claims.

ii. Set the case-sensitive attributes as follows:

1. Change givenname to firstName: Required. user.givenname
2. Change surname to lastName: Required. user.surname
3. homeCID: Optional. For CrowdStrike Flight Control environments. Name of the CID

If you manage all your users with one IdP, it's best to use a mapping of the IdP-based user groups, such as AD groups, for the CID instead of a static CID assignment.

b. Optional. For the Falcon user roles and the Falcon Flight Control user groups, complete these steps.

Note: Follow these steps for one or more roles—or one or more user groups. Don't use these steps with a combination of roles and user groups.

- i. Create an Entra group for the role or Flight Control user group.
- ii. Add users that require that role or user group to the Entra group.
- iii. Map the Entra group to the ID for the Falcon role or the ID for the Falcon Flight Control user group.
 1. Go to the application registration for Falcon SSO in Entra ID > App registrations.
 2. Create an Entra app role for the Falcon role or Flight Control user group.

Falcon Management

- Set Allowed member types to Users/Groups
- Set Value to the ID for the Falcon role or the ID for the Flight Control user group.

You can specify the IDs for multiple roles or the IDs for multiple user groups, separated by commas.

To get the ID for a role, you have these options:

- Use an API endpoint

The endpoint to use is: GET /user-management/queries/roles/v1

For more info, see Users and Roles APIs.

- Use the Falcon console

Go to **Host setup and management > Falcon users > Roles and permissions**. Find the role you want the ID for. Click  for that role and select **View role details**. Look at your browser's address bar. The ID is in the URL, .../roles-and-permissions/<role_ID>/permissions, shown by the <role_ID> value.

To get the ID for a Flight Control user group, you have these options:

- Use an API endpoint

For more info, see <https://assets.falcon.crowdstrike.com/support/api/swagger.html#/mssp/queryUserGroups>.

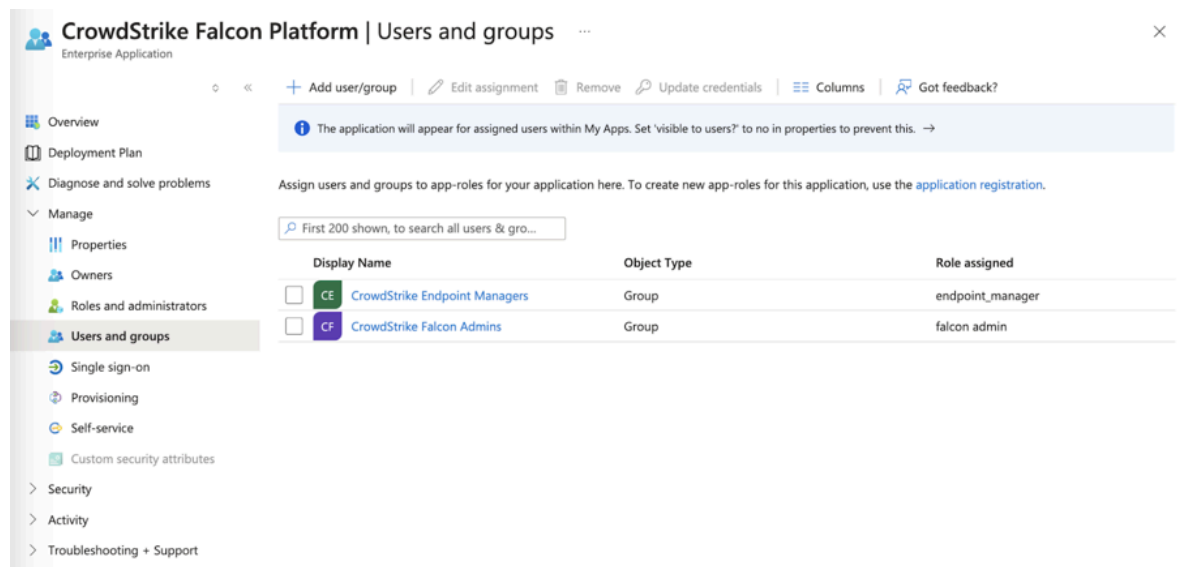
- Use the Falcon console

Using the parent CID, go to **Host setup and management > Flight Control management > User groups**. Find the user group you want the ID for. Click  for that group and select **View user group**. Look at your browser's address bar. The ID is in the URL, .../roles-and-user-groups/<group_ID>/users, shown by the <group_ID> value.

iv. Assign the Entra group to the Enterprise Application.

1. Go to **Entra ID > Enterprise Applications > Falcon Platform app > Users and groups**.
2. Select the Entra group that you want to assign to the application.
3. Select the Falcon role or Flight Control user group you want to assign to the Entra group.

For example, the following image shows 2 roles available to select.



v. Add a custom SAML attribute to include the mapped role or user group.

1. In your single sign-on application SAML setup, select to edit **User Attributes & Claims**.
2. For Falcon roles:
 - a. Add a new claim.
 - b. Set the name to `roles`.
 - c. Add the source attribute as `user.assignedroles`.

With the claim added, the SAML assertion includes each Falcon role in a comma-delimited array.

When you finish, the SAML Attributes and Claims configuration should look similar to the following image.

1

Basic SAML Configuration

 Edit

Identifier (Entity ID)	https://falcon.crowdstrike.com/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://falcon.crowdstrike.com/saml/acs
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2

Attributes & Claims

 Edit

emailaddress	user.mail
firstName	user.givenname
name	user.userprincipalname
lastName	user.surname
roles	user.assignedroles
Unique User Identifier	user.userprincipalname

3. For Flight Control user groups:

a. Create a group called `Flight Control - <group_ID>`.

The group ID must be in the name of the group.

b. Assign users to the group and assign the group to the Falcon SSO Enterprise Application.

c. Add a new group claim.

d. Select Groups assigned to the application.

e. Set Source attribute to Cloud-only group display names.

f. In Advanced options, select Customize the name of the group claim.

i. For Name, enter `userGroups`.

ii. Select Apply regex replace to groups claim content.

1. Enter a regex pattern to match the Flight Control group name.

For example, the following pattern filters for groups with a `Flight Control -` prefix and stores the group ID in a capture group:

```
^Flight Control - (? 'groupId' [a-fA-F0-9]{32})
```

2. Use the capture group defined in the previous step in Regex replacement pattern.

In this case, `{groupId}`.

3. Click Save.

When you finish, the Group Claims configuration should look similar to the following image.

Group Claims



Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- ☐ None
- ☐ All groups
- ☐ Security groups
- ☐ Directory roles
- ☒ Groups assigned to the application

Source attribute *

Cloud-only group display names

☐ Emit group name for cloud-only groups ⓘ

^ Advanced options

☐ Filter groups

Attribute to match

Match with

String

☒ Customize the name of the group claim

Name (required)

userGroups

Namespace (optional)

☐ Emit groups as role claims ⓘ

☒ Apply regex replace to groups claim content

Regex pattern * ⓘ

^Flight Control - (? 'groupId'[a-zA-Z0-9]{32})

Regex replacement pattern * ⓘ

{groupId}

☐ Expose claim in JWT tokens in addition to SAML tokens

Save

Step 2: Contact us to configure Falcon SSO for your organization

To configure Falcon to communicate with your IdP, contact Support using the [CrowdStrike Customer Center](#). For our support team to complete your SSO request, you must have the role Falcon Administrator or Intel Application Admin.

1. Log in to the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, log in to the [CrowdStrike Government Customer Center](#).
2. Create a new ticket titled Request for SSO integration.
3. If you are using Just-in-Time (JIT) provisioning, mention that in the ticket. Also, request that JIT trial mode be set.

Falcon Management

4. Upload your IdP's SAML metadata XML to the ticket. The metadata XML file contains these required attributes:

- o Entity ID (usually in the form of a URL)
- o Redirect URL
- o Public certificate
- o Supported bindings

Our support team receives your ticket and provides you with status updates as needed.

Step 3: Test logging in with SSO

After our support team configures your organization to use SSO, we notify you through the CrowdStrike Customer Center. At this point, your Falcon environment is in "onboarding mode."

In onboarding mode, Falcon's login screen accepts your Falcon credentials by default. You can also use a specific URL to log in with your SSO credentials instead. Onboarding mode is intended for temporary use while you test your SSO credentials.

To log in with SSO while in onboarding mode:

1. Open the SSO login URL in a supported browser. Check the domain for your Falcon console and use the following URL with the matching domain:

- o US-1: <https://falcon.crowdstrike.com/login/sso>
- o US-2: <https://falcon.us-2.crowdstrike.com/login/sso>
- o EU-1: <https://falcon.eu-1.crowdstrike.com/login/sso>
- o US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/login/sso>
- o US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/login/sso>

2. Enter your email address in the Email field.

3. Click Continue, and the Falcon console redirects you to your IdP's authentication process.

4. Authenticate using your SSO credentials.

Note: After you exit onboarding mode, you can log in to Falcon at its usual URL. However, the SSO login URL remains available after you exit onboarding mode.

Step 4: Transition to SSO authentication

After you've successfully tested an SSO user, you're ready to exit "onboarding mode" and authenticate only through SSO.

Important: After this step, no one in your organization can log in with their Falcon credentials. Be sure that:

- Everyone in your organization understands how to log in with SSO using a supported browser
- Your organization's SSO accounts are granted access to the Falcon application in your IdP

To transition to SSO (and disable authentication with Falcon credentials):

1. Log in to the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, log in to the [CrowdStrike Government Customer Center](#).
2. Create a new ticket titled Request to exit SSO onboarding mode.

Note: If you were using Just-in-Time trial mode and have also confirmed the configuration there, request that it be disabled.

Our support team receives your ticket and notifies you when the transition to SSO is complete.

When you exit onboarding mode, you can log in either:

- Through the Falcon console: Using a supported browser, go to your [Falcon console URL](#). When you enter your email address, you're prompted for SSO authentication.
- Through your IdP: Using a supported browser, log in to your IdP's interface and select your Falcon application.

Update your SSO configuration to use Just-in-Time provisioning

If you're already using SSO as described in [Set up and use SSO](#), you may want to enable Just-in-Time provisioning so that your users who log in to the Falcon console using the IdP-initiated login link get Falcon accounts created automatically. To enable this provisioning, you need to add some SAML attributes to your IdP configuration.

Important: System for Cross-domain Identity Management (SCIM) is not supported with Just-in-Time provisioning.

If you update your configuration, use trial mode to verify your changes work as expected:

1. Enable trial mode by contacting Support using the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, contact [CrowdStrike Government Customer Center](#).
2. While in trial mode, use audit logs to verify assertions. For more info about auditing, see [Auditing](#).
3. Disable trial mode by contacting Support using the [CrowdStrike Customer Center](#). For US-GOV-1 and US-GOV-2 customers, contact [CrowdStrike Government Customer Center](#).

To update your configuration to use Just-in-Time provisioning, focus on the Just-in-Time provisioning steps in the section for the IdP you're using:

- [Active Directory Federation Services \(AD FS\)](#)
- [Okta](#)
- [PingFederate](#)
- [PingOne](#)
- [Microsoft Entra ID](#)

After you update your IdP configuration, continue to [Step 2: Contact us to configure Falcon SSO for your organization](#).

Falcon Management

Auditing

You can see a history of the SAML SSO assertions that IdPs have sent to CrowdStrike by looking at the Falcon UI audit log.

To see this audit log:

1. Go to Audit logs > Falcon UI.
2. Set Service to CS Authentication.
3. Set Action to SSO.

Be aware that the custom assertions might not be fully honored because, for example, a role or user group does not exist or a user is not allowed to have a certain role.

For Just-in-Time (JIT) provisioning, if you are in trial mode, the custom assertions are not honored, but you can verify that the expected assertions are received by CrowdStrike.

Troubleshooting

Issue: Can't log in with SSO

Check these possible causes in this order:

1. Make sure the user account exists in Falcon.
2. Make sure the user account's SSO username exactly matches their Falcon email address.
3. Make sure the user is provisioned in your IdP to use the application you created for Falcon.
4. Make sure your IdP application uses the correct Falcon metadata XML attributes. Check the domain for your Falcon console and use the following URL with the matching domain:
 - o Service Provider Entity ID:
 - US-1: <https://falcon.crowdstrike.com/saml/metadata>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/metadata>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/metadata>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/metadata>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/metadata>
 - o Single Sign-On URL or Security Token Consumer URL:
 - US-1: <https://falcon.crowdstrike.com/saml/acs>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/acs>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/acs>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/acs>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/acs>
 - o Name ID Format: the user's email address as shown in Falcon
 - o Public Certificate: The certificate information provided at:
 - US-1: <https://falcon.crowdstrike.com/saml/metadata>
 - US-2: <https://falcon.us-2.crowdstrike.com/saml/metadata>
 - EU-1: <https://falcon.eu-1.crowdstrike.com/saml/metadata>
 - US-GOV-1: <https://falcon.laggar.gcw.crowdstrike.com/saml/metadata>
 - US-GOV-2: <https://falcon.us-gov-2.crowdstrike.mil/saml/metadata>
5. Contact Support through the [CrowdStrike Customer Center](#) to validate your IdP details. The information you provide to support must exactly match the information given by your application in your IdP, including these required attributes:
 - o Entity ID (usually in the form of a URL)
 - o Redirect URL
 - o Public Certificate
 - o Supported bindings

FIDO Two-Factor (2FA) Authentication

Fast Identity Online (FIDO) two-factor authentication offers improved ease-of-use and stronger protection against phishing and other social engineering attacks.

Overview

The Falcon console supports Fast Identity Online (FIDO) two-factor authentication, offering improved ease-of-use and stronger protection against phishing and other social engineering attacks.

Falcon Management

Requirements

- Subscription: Supported with all subscriptions
- Sensor: All supported sensor versions
- System requirements: FIDO2-certified devices, such as Touch ID or YubiKey
- Default roles: Falcon Administrator
- CrowdStrike clouds: Available in all clouds

Understanding FIDO two-factor authentication (2FA)

Fast IDentity Online (FIDO) devices use hardware or biometrics for authentication, offering strong protection against phishing and ease of use, improving on time-based one-time passwords (TOTP), which can be vulnerable to phishing attacks.

CrowdStrike's FIDO two-factor authentication lets you use FIDO2 devices to authenticate, in addition to TOTP devices. Once enabled for your CID, your users are prompted for FIDO authentication after entering their username and password. CrowdStrike supports all FIDO2-certified devices, such as YubiKey and Touch ID.

As an admin, you can also configure which factors are allowed for two-factor authentication, such as TOTP and FIDO devices or FIDO devices only.

Note: FIDO authentication is not supported for RTR actions. If you want to use two-factor authentication for RTR actions, you need to continue to use TOTP in addition to FIDO. Although you can set up FIDO alongside single sign-on, SSO users won't be prompted for an additional FIDO authentication challenge.

Setup Overview

The steps to a successful FIDO rollout for your organization include having one or more FIDO-certified devices to register and communicating the FIDO enrollment plan to your end users, as well as whether you're using FIDO by itself or alongside time-based one-time password (TOTP) authentication.

Setting up MFA FIDO includes these general steps.

- [Step 1: Develop a FIDO implementation plan.](#)
- [Step 2: Register one or more FIDO devices.](#)
- [Step 3: Enable FIDO for your CID.](#)
- [Step 4: Inform your users.](#)
- [Step 5: Test your FIDO setup by logging in.](#)

When your users next log in to the Falcon console, they are prompted to enroll a FIDO device for authentication.

Step 1: Develop a FIDO implementation plan

Enabling FIDO for your organization changes the login experience for the end users in your CrowdStrike account. It's important to communicate this change before enabling FIDO for your organization.

Here are some things to keep in mind:

- If you're already using TOTP for authentication, are you using FIDO alongside that or as a replacement?
- Do all of your end users have FIDO2-certified devices?
- What's your plan for monitoring the rollout of FIDO devices across your organization's users and determining when that's complete?

Note: If an end user doesn't have a FIDO device, TOTP can be used as a fallback option, if you have TOTP enabled for your CID.

Step 2: Register one or more FIDO devices

Before you can enable FIDO for your organization, you need to register one or more keys, or FIDO devices, to use for authentication. You need to register at least one device before you turn FIDO authentication on.

1. Go to User profile > Account security.
2. Under Security keys, click Add.
Note: : You may be prompted to re-authenticate with an existing device before adding or modifying a device.
3. Register a FIDO device, such as a Yubikey or Touch ID.
4. Optional. Set a device nickname.

Note: If you don't have a TOTP or FIDO device registered, you are prompted to register a device on log in. By default FIDO is presented if your organization allows it, but you can fall back to TOTP.

Step 3: Enable FIDO for your CID

Once you've registered one or more devices for FIDO two-factor authentication for your organization, follow these steps to enable it for use as a login option.

1. Go to Support and resources > General settings > Security > Multi-factor authentication.
2. Set WebAuthn with FIDO2 security key to On.
3. Optional. If you are not planning on using TOTP for authentication, you can disable it.

Step 4: Inform your users

Inform your users that FIDO is enabled based on your implementation plan.

Note: If you have TOTP enabled, your users can continue to use that until you've disabled TOTP for your CID.

Falcon Management

Step 5: Test your FIDO setup by logging in

Confirm your FIDO two-factor authentication has been successfully enabled for your CID and register a FIDO device for your admin.

1. Log out of the console.
2. Go to [CrowdStrike login](#).
3. Log in with your username and password.
4. On the Verify your identity page, click Use security key, and then use your device to finish logging in.

Once you've tested and verified your FIDO two-factor authentication, follow your plan to inform your end users that FIDO is available.

Note: If your log in fails or you lost your authentication device, then register a new FIDO or TOTP device.

Review users and their registered 2FA factors

Confirm your FIDO two-factor authentication has been successfully enabled for your CID and register a FIDO device for your admin.

1. Log out of the console.
2. Go to [CrowdStrike login](#).
3. Log in with your username and password.
4. On the Verify your identity page, click Use security key, and then use your device to finish logging in.

Once you've tested and verified your FIDO two-factor authentication, follow your plan to inform your end users that FIDO is available.

Note: If your log in fails or you lost your authentication device, then register a new FIDO or TOTP device.

Export your user activity

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Click [Export > CSV](#).
3. Download the exported CSV file.

Recover lost two-factor authentication access

Note: When you restore access for someone, make sure to verify that they are who they say they are. For more info, see [NIST Digital Identity Guidelines](#).

If a user loses access to TOTP and their FIDO devices, follow these steps to reset the user's access and enable that user to register new TOTP and FIDO authentication factors.

1. Go to [Host setup and management > Falcon users > User management](#) .
2. Next to the user whose authentication you want to reset, click the  Open menu, and then click [Reset MFA](#).
3. At the confirmation prompt, click [Send request](#).
4. When the user logs in again, the user is prompted to register a new FIDO device.

Note: As an admin, you cannot reset your own TOTP or FIDO two-factor authentication access. Contact CrowdStrike support for assistance.

Falcon Flight Control and Multi-CID Support

For a Falcon Flight Control or multi-CID account, leverage a parent/child hierarchy to efficiently manage policies, API access, and respond to detections.

Overview

With a Falcon Flight Control (formerly known as MSSP) or multi-CID account, CIDs are arranged in a parent/child hierarchy. Through one parent CID you can manage separate child CIDs, including managing policies, responding to detections, and managing API access.

From the parent CID, you can:

- View and respond to detections for all child accounts
- Manage global policies for all child accounts:
 - File integrity policies
 - Mobile policies
 - Prevention policies
 - Data Protection policies
 - Real Time Response (RTR) policies
 - Sensor update policies
 - Device Control policies
- Manage users for each child account
- Manage API clients and keys
- Add and manage child CIDs

From a child CID, users can:

- Monitor and respond to detections for their specific child CID
- Manage local policies for their specific child CID
- Manage users for their specific child CID

Falcon Management

Understanding Falcon Flight Control vs. multi-CID accounts

Falcon Flight Control partners

Falcon Flight Control provides cybersecurity management and monitoring of security systems and devices to outside customers. Separate customer accounts are connected to a single Flight Control account that provides these services for them, reducing the end-customer's need to have on-site cybersecurity personnel to keep them protected from attacks and other threats.

Multi-CID customers

A multi-CID customer consists of multiple departments or divisions in separate child CIDs; however, they are all a part of one large organization. For example, separate accounts might be needed for a healthcare division, finance division, and IT division.

Supported subscriptions

- Falcon Data Protection
- Falcon Device Control
- Falcon Discover
- Falcon Exposure Management
- Falcon FileVantage
- Falcon for Mobile
- Falcon Identity Protection. For more info, see [Falcon Flight Control support](#).
- Falcon Insight XDR
- Falcon Next-Gen SIEM. For more info, see:
 - Falcon Flight Control for cases
 - Falcon Flight Control for case management
 - Falcon Flight Control for third-party data connections
- Falcon Overwatch
- Falcon Prevent
- Falcon Spotlight

Provisioning child CIDs using the Falcon console

Parent CIDs can add new child CIDs and manage their product subscriptions directly in the Falcon console at [Host setup and management > Flight Control management > CID provisioning overview](#).

Requirements

To provision child CIDs and manage their provisioning settings in the Falcon console, you must meet these requirements:

- Subscription: Available for Falcon Flight Control partners with self-service provisioning enabled on the parent CID.
- Feature enablement: The parent CID must be fully onboarded and self-service provisioning must be enabled. To enable self-service provisioning, contact your Alliances Rep and Solution Architect, who will verify eligibility and enable access.
- Default roles: Requires one of these roles:
 - Falcon Administrator
 - Provisioning Admin
- Permissions required for custom roles:
 - Permission group: Flight Control
 - Requires these permissions to create and manage child CIDs:
 - Edit CID products
 - Create CID
 - Update CID
 - Requires these permissions to view provisioning transactions, statuses, and the audit log:
 - List provisioned CIDs
 - List transactions
 - Read provisioning status
 - Read transactions
 - Read CID provisioning details
- Child CID limit: A parent CID can have a maximum of 200 child CIDs. To request a higher limit, contact Support.
- CrowdStrike clouds: Available in US-1, US-2, and EU-1

Add a new child CID

1. Verify that you meet the necessary prerequisites. For more info, see [Requirements](#).
2. In the Falcon console, go to [Host setup and management > Flight Control management > CID provisioning overview](#).
3. Click Add CID.
4. In the Add CID dialog, select whether you want the CID to start as a Trial or Paid account.
Note: You can convert trial accounts to paid status at any time, but paid accounts cannot change to trial.
5. Enter the customer and CID information in the required fields.
6. In the Add users to CID section, select Yes or No for these options:
 - a. Create a new admin and assign it to this CID.
 - b. Allow additional email domains for future users.
7. If you selected "yes" for either option, click Next and enter the admin information and/or additional email domains.
8. Click Submit.

Check provisioning status

You can check a CID's provisioning status on the CID provisioning queue tab at [Host setup and management > Flight Control management > CID provisioning overview](#).

Falcon Management

Multi-CID accounts

If you're a new or existing multi-CID customer or interested in learning more about our multi-CID offering, contact your sales team.

Managing child CIDs

Parent CIDs can manage child CIDs from within the Falcon console at [Host setup and management > Flight Control management > CID provisioning overview](#) . For accounts with a 3-tier architecture, grandparents can manage parents and switch into a parent CID to manage its child CIDs. For more info, see [Switch CIDs](#).

You can perform these actions:

- Add new child CIDs under a parent CID
- Add or remove CrowdStrike product subscriptions for child CIDs
- Change a child CID's status
- View child CID details
- Search for child CIDs by name or ID
- Filter child CIDs by status

Note: Changes can take up to 30 minutes to appear in the Falcon console.

Provisioning actions are recorded on the Audit log tab at [Host setup and management > Flight Control management > CID provisioning overview](#) .

Switch CIDs

You can switch to a child CID directly from the CID provisioning overview table at [Host setup and management > Flight Control management > CID provisioning overview](#) . On the CID that you want to switch to, click Open menu  and select Switch to CID.

Add products to a child CID

You can add new product subscriptions to a child CID at any time. Before you begin, verify these requirements are met:

- The parent CID has active subscriptions for the products you want to add.
- The child CID status is Paid or Trial. Suspended CIDs must be converted to Paid before you can modify product subscriptions. For more info about CID statuses, see [Change a child CID's status](#).

Note: Some products cannot be added from the Falcon console. To add these products, contact Support.

1. Go to [Host setup and management > Flight Control management > CID provisioning overview](#) .
2. On the CID that you want to add new products to, click Open menu  and select Add products.
3. In the Search for products field, type the product name or select it from the list.
4. Click Save.

Remove products from a child CID

You can remove products from child CIDs in Paid or Trial status. Suspended CIDs must be converted to Paid before you can modify their product subscriptions. For more info about CID statuses, see [Change a child CID's status](#).

1. Go to [Host setup and management > Flight Control management > CID provisioning overview](#) .
2. On the CID that you want to remove products from, click Open menu  and select Remove products.
3. In the Search for products field, type the product name or select it from the list.
4. Click Save.

Change a child CID's status

You can view and change child CID statuses at [Host setup and management > Flight Control management > CID provisioning overview](#) . The CID status column shows each CID's current status.

CID statuses:

- Paid: The CID is provisioned with active, paid product subscriptions.
- Suspended: The CID's Falcon console access is blocked, but the CID is not deprovisioned. All customer data is retained and becomes accessible when the CID is converted to Paid status.
- Trial: The CID is provisioned with product subscriptions in a free trial period. After 15 days, Trial accounts automatically convert to Paid status.

1. Go to [Host setup and management > Flight Control management > CID provisioning overview](#) .
2. On the CID that you want to remove products from, click Open menu  .
3. Select one of these options:
 - a. Convert to paid: Use this option when the CID is in Trial or Suspended status and you want to activate or reactivate their Paid status.
 - b. Suspend: Use this option to temporarily block Falcon console access while retaining account data.

View child CID provisioning details

View provisioning details for your child CIDs, including CID name, provisioned date, CID status, and current product subscriptions.

By default, the list is sorted by Provisioned date with the most recent date first. You can search by CID name, filter by status, or sort by clicking the CID name or Provisioned date column headers. Click a header again to reverse the sort order.

1. Go to [Host setup and management > Flight Control management > CID provisioning overview](#) .

Falcon Management

2. Click a child CID row to open the details panel and view additional info including CID ID, number of hosts, allowed domains, and transaction details with direct access to the CID's provisioning queue.
3. Optional. To view any ongoing operations in the provisioning queue, in the Transaction details section, click View details. The results shown in the CID provisioning queue are filtered for the relevant CID. For more info, see [Track operations in the CID provisioning queue](#).

Track operations in the CID provisioning queue

Each provisioning action, such as creating a new child CID or modifying product subscriptions, is assigned a unique operation ID. To view these operations, go to [Host setup and management > Flight Control management > CID provisioning overview](#) and click CID provisioning queue. The queue displays all In progress and Failed actions from the last month.

From the CID provisioning queue tab, you can perform these actions:

- Search for child CIDs by CID name, ID, or operation ID
- Filter by provisioning status
- View operation details
- Retry failed operations

Tip: Hover over a Failed provisioning status to see what caused the failure.

Review the provisioning audit log

All provisioning activity is recorded in the Audit log tab at [Host setup and management > Flight Control management > CID provisioning overview](#) . You can filter events by time, activity, or actor type to review historical CID provisioning activity.

Provisioning child CIDs using the Partner Portal

Important: Child CID provisioning through the Partner Portal will be deprecated in a future release. We recommend provisioning using the Falcon console or the CrowdStrike API instead. For more info, see [Provisioning child CIDs using the Falcon console and ../uncategorized/user-guides/provisioning_apis.html](#).

Flight Control users with [CrowdStrike Community Partner portal](#) access can continue using it to provision new child CIDs. This provisioning method is still available, but we recommend transitioning to the Falcon console or the CrowdStrike Provisioning API to maintain continuity.

To add a new child CID using the partner portal:

1. Log in to the CrowdStrike Community Partner portal.
2. Click the My CS Business menu, then click Provision End Customer.
3. Enter your customer's details.
4. Select the parent CID that the child CID should be assigned to.
5. Under Products, select the CrowdStrike products the child CID needs.
6. Click Submit.

The new child CID is provisioned to your parent CID shortly after submitting the request. To view the completion status, click the My CS Business menu, then click Provision Transaction Monitoring.

Note: Child CIDs provisioned through the Partner Portal can take up to 24 hours to appear in the Falcon console.

Managing policies

Global policies (Falcon Flight Control)

Centrally define and manage different types of policies for all of your child CIDs from your parent CID. The policies you can manage include prevention, sensor update, mobile, file integrity, device control, and RTR policies. After a policy is created and enabled in the parent CID, it becomes available across your environment so you can assign them to host groups in respective child CIDs.

As a user in a child CID, you can see which policies are managed by your Flight Control parent CID. These policies are labeled with Global Admin next to each policy's precedence.

Policies follow the same precedence set in the parent CID as they're assigned to host groups in child CIDs.

For Device Control policies only, you can enable or disable policy propagation from parent to child CIDs from within a policy. Select the Policy propagation checkbox under Setting name to enable or disable this feature.

Note: If you disable policy propagation, your existing child host group assignments remain. When you re-enable policy propagation, these assignments automatically become active again.

For more info about managing policies, read our [policy management guides](#):

- [Detection and Prevention Policies](#)
- [Configure Falcon Data Protection](#)
- [Configuring Falcon for Mobile](#)
- [Sensor Update Policies](#)
- [Real Time Response](#)
- [Network Containment](#)
- [Falcon FileVantage](#)
- [Device Control](#)

Falcon Management

Local policies

At the child CID level, local policies can be created that are only available in the child CIDs they're created in. Local policies should be created for things that shouldn't be managed across all child CIDs, as they are specific to individual child CIDs. In addition to prevention, sensor update, device control, and RTR policies, other types of policies can be managed in each child CID:

- [Response Scripts & Files](#)
- [Containment policies](#)
- [USB Device Control policies](#)
- [File exclusions](#)
- [Prevention hashes](#)
- [Manage Data Protection policies](#)
- [Mobile policies](#)
- [General settings](#)
- [FileVantage policies](#)

Note: If you only want to manage policies at the global level, we recommend not giving child CID users roles that allow them to create and manage policies.

You can create local policies to override global ones. For example, you might have several prevention policies defined at the parent CID level that are applied to your child CIDs. However, one child CID requires a separate policy with a higher precedence. Any policies you create in that child CID automatically have a higher precedence than the global policies inherited from the parent CID.

Local policies cannot be managed from the parent CID. As you create local policies in your child CIDs, assign them to host groups you've created in each child CID.

Managing detections

You can view, search, and manage endpoint, mobile, and identity-based detections for all your child CIDs from the parent CID.

Note: While you can manage Device Control policies for child CIDs from a parent CID, viewing child Device Control activity from a parent is not supported.

Viewing detections

You can see detections for all your child CIDs aggregated on one page, letting you easily search through detections without switching to different child CIDs. From this aggregated view, you can see which child CID they're coming from in the detection details. If you're interested in only viewing detections for one or more specific child CIDs, use the Customer filter in the filter bar at the top of the screen to filter detection results.

Assigning detections

You can assign detections for any CID in your environment to which you've been given access with the proper permissions. From the parent CID, you can manage multiple detections at the same time, even from different child CIDs. When one or more detections are selected from the same child CID, the list of assignees includes users in your parent CID and users who have access to that child CID with a role for managing detections. If multiple detections are selected from different child CIDs, only users who have access to manage detections in all of those child CIDs will display in the list of assignees.

When working directly in a child CID, the list of assignable users includes anyone with access to the CID and a role with permissions for managing detections.

Note: For security purposes, to see a user in the assignee list, you must have access to the user's home CID with role permissions that allow you to view users in that CID.

Mobile detection exclusions

Mobile detection exclusions that are created in a parent CID are applied to the parent CID and all the child CIDs. You can create these exclusions from mobile detections generated within the parent CID or from aggregated mobile detections. Aggregated detections appear in the parent CID based on your configuration and include detections across child CIDs.

You can delete inherited exclusions in a child CID if they're not needed. If you need to add the exclusion back, you can do so locally in the child CID. You can also remove and then re-add the exclusion from the parent CID, however, this would propagate the exclusion to any other child CIDs that might have locally removed the original inherited exclusion.

Mobile detection exclusions that are created in a child CID don't appear in the parent CID and are fully managed in the child CID. Local exclusions take precedence over globally inherited exclusions.

Note: Endpoint detection exclusions and identity-based detection exclusions aren't propagated from the parent CID to child CIDs.

Managing hosts

Get an integrated picture of hosts across your entire environment of child CIDs from the parent CID view of the [Host Management page](#) (Host setup and management > Manage endpoints > Host management). This unified view allows for efficient visualization and management of all your hosts in one place. See a summary of key information at a glance for all hosts, the hosts in a child account, or individual hosts. You can quickly skim host details or drill down to get even more granular info and take appropriate actions.

Flight Control gives you all of the features described in the [Host Management guide](#), plus additional capabilities designed to help you easily take care of essential host management tasks in your child accounts.

- **Customer filter:** Use the Customer filter to focus on hosts in specific child accounts. Click a child CID name to switch from displaying the full list of hosts to a breakdown of hosts in the selected child CID.
- **Customer column:** In the hosts list, the Customer column shows the CID name associated with each host. This additional level of reference makes it easy to identify and view the hosts you're interested in.

Migrating hosts between CIDs

Migrate hosts from one CID to another by creating migration jobs in a Falcon Flight Control parent CID. This is useful to help scale with organizational needs or business operational changes. When a host is migrated, its sensor is reprovisioned in the destination CID. A host reboot is not required.

Important: You can only migrate between CIDs that are managed by parent CID where you create the migration job. Additionally, the original CID and destination CID must be in the same CrowdStrike cloud and must share at least one domain in common. See [Host migration CID domain requirements](#).

Existing detections and telemetry are not migrated, they stay associated with the existing host record in the original CID. After migration, only new detections and telemetry appear in the destination CID for a migrated host.

Note: Host migration is only available from the updated Host management page of the Falcon console.

Falcon Management

Host migration requirements

Subscription: Falcon Flight Control

Sensor support:

- Falcon sensor for Windows 7.17 and later
Note: Host migration is supported on hosts running Windows 7/2008 R2 only when using 7.16.18616
- Falcon sensor for Mac 7.16 and later
- Falcon sensor for Linux 7.16 and later
Important: Host migration isn't supported for DaemonSet deployments of Falcon sensor for Linux.

Default roles: Falcon Administrator

Understanding host migration

Hosts are migrated using host migration jobs. You can create multiple migration jobs. Each migration job includes one or more hosts migrating to the same destination CID. Migration jobs are managed in the migration queue.

This flow details the migration process:

- Create a host migration job:** Specify one or more hosts to migrate, specify the destination CID, and assign static host groups to hosts, if desired.
- Managing the host migration queue:** Monitor the progress, view the status, and open the migration job details page of one or more migration jobs. Start, cancel, or delete migration jobs. Export the results of a finished job.
- Managing a host migration job:** View migration job details, change the job name, cancel or delete the migration. For each host, view migration status and events, manage static host group assignments, and remove them from the job. Start, cancel, or delete the job. Export the results of a finished job.

Important: You can only migrate between CIDs that are managed by parent CID where you create the migration job. Additionally, the original CID and destination CID must be in the same CrowdStrike cloud and must share at least one domain in common. See [Host migration CID domain requirements](#).

Migration process overview

These actions and configurations are included in a successful host migration:

- Sensor version:** Migrated hosts remain on the same sensor version.
- Installation tokens:** If the destination CID requires an installation token, a token is automatically created for the migration job using a naming convention that starts with host-migration.
- Host ID:** Migrated hosts are assigned a new host ID in the destination CID.
- Grouping tags:** Falcon sensor tags and Falcon grouping tags assigned to a host are retained after migration to the destination CID, ensuring they are added to the appropriate host groups and prevention policies are correctly applied.
Note: Currently, Falcon sensor grouping tags for Linux hosts are not migrated.
- Host groups:** Migrated hosts are automatically included in applicable dynamic host groups. Static host groups for the destination CID can be assigned to each host in a migration job before it's started.
- Sensor update policies:** Sensor update policies for a migrated host are assigned according to destination CID settings and destination CID host group membership.
- Host record in original CID:** The host record in the original CID is retained, with the original host ID, and any past detections and telemetry, for the duration of the host retention period. This retention period is 45 days.

Note: If migrating a Linux host from a CID that has FileVantage to a CID without FileVantage, the Falcon sensor for Linux doesn't stay in kernel mode.

Host migration CID domain requirements

You can only migrate hosts between CIDs that are managed by the same parent CID and that are in the same CrowdStrike cloud. Additionally, there must be one domain in common between all original CIDs and the destination CID of a migration job.

If you don't see the desired destination CID in the list of available options when creating a migration job, it's because it doesn't share a domain in common with the original CIDs of the hosts you have selected for the job.

To view available domains for a CID, go to [Support and resources > Resources and tools > General settings](#) , then click the CID details tab and view the Domains allowed list.

For more details, refer to these examples:

Example 1: In this example, the desired destination CID shares the domain exampleC.com with both original CIDs.

Note: The destination CID does share the domain exampleB.com with Original CID 1, but original CID 2 doesn't share that domain so it doesn't satisfy the domain requirement.

CID	CID domains
Original CID 1	exampleA.com exampleB.com exampleC.com
Original CID 2	exampleC.com exampleD.com
Destination CID	exampleB.com

Falcon Management

exampleC.com
exampleE.com

Example 2: In this example, the desired destination CID doesn't share a domain in common with the original CIDs. As a result, the desired destination CID doesn't appear in the list of available destination CIDs when creating a migration job.

CID	CID domains
Original CID 1	exampleA.com exampleB.com exampleC.com
Original CID 2	exampleC.com exampleD.com
Destination CID	exampleB.com exampleD.com exampleE.com

Example 3: In this example, the desired destination CID shares a domain in common with Original CID 1 and a different domain in common with Original CID 2, but Original CID 1 and Original CID 2 don't share a domain in common. As a result, the desired destination CID doesn't appear in the list of available destination CIDs when creating a migration job.

CID	CID domains
Original CID 1	exampleA.com exampleB.com exampleC.com
Original CID 2	exampleD.com exampleE.com
Destination CID	exampleB.com exampleD.com

Example 4: In this example, the desired destination CID shares a domain in common with Original CID 1 and a different domain in common with Original CID 2. Additionally, Original CID 1 shares a domain in common with Original CID 2. However, there is not a domain that is shared between Original CID 1, Original CID 2, and the desired destination CID. As a result, the desired destination CID doesn't appear in the list of available destination CIDs when creating a migration job.

CID	CID domains
Original CID 1	exampleA.com exampleB.com exampleC.com
Original CID 2	exampleC.com exampleD.com
Destination CID	exampleB.com exampleD.com

Create a host migration job

1. Sign into the parent CID and go to the Host Management page, [Host setup and management > Manage endpoints > Host management](#) .
Note: Host migration is only available from the updated Host management page.
2. Select one or more hosts to migrate and then click [Migrate selected hosts](#).
Note: The maximum number of hosts allowed for a migration job is 1,000.
3. In the Migration setup dialog, specify this info, and then click Next.

Falcon Management

- Migration job name: Enter a name for the migration job. You can monitor this job in the host migration queue after it's created.
- Destination CID: Select the CID you want to migrate the selected hosts to.

Important: If you don't see the desired destination CID in the list of available options when creating a migration job, it's because it doesn't share a domain in common with the original CIDs of the hosts you have selected for the job. See [Host migration CID domain requirements](#).

- Assign to static host groups before migration: Select to assign hosts to static host groups in the destination CID. If you select this option, you can assign static host groups to each host before starting the migration job.

Important: Migrated hosts are automatically included in qualifying dynamic host groups in the destination CID, regardless of whether they are manually assigned to static host groups. For more info about host groups, see [Managing host groups](#).

4. Start the migration job:

- Optional. If you selected Assign to static host groups before migration, the new migration job details page opens. Use one of these methods to assign static host groups to the hosts in the destination CID, and then start the migration job:
 - a. Select the desired hosts and click Assign static host groups.
 - b. In the Assign static host groups dialog, select the desired static host groups in the destination CID, and then click Assign.
 - c. After static host groups have been assigned, click Start migration.
Note: If a migration job is created but not started, it's removed from the migration queue after 45 days.
- If you didn't select Assign to static host groups before migration, in the Confirm migration dialog, click Migrate.

Managing the host migration queue

Migration jobs that have been created appear in the migration queue. Go to [Host setup and management > Manage endpoints > Host management](#) , then click Host migration queue.

In the host migration queue, you can view the progress and status of current host migration jobs and you can view a history of completed, failed, or partially failed migration jobs for up to 45 days.

Migration job status

Each migration job in the migration queue is displayed with one of these statuses:

- Created: Created but not started. If a migration job was created and the Assign to static host groups before migration option was selected, it appears in a Created state so you can assign static host groups in the destination CID. After assigning static host groups, click Start migration.
Note: If a migration job is created but not started, it's removed from the migration queue after 45 days.
- Active: The hosts in the migration job are actively being migrated
- Completed: All hosts in the migration job have been successfully migrated
- Canceled: The migration job has been manually canceled using the Cancel action.
- Partially Failed: The migration job has finished. At least one host was successfully migrated but not all hosts in the job were successfully migrated. Open the migration job to view hosts with a status of Failed for troubleshooting. See [Troubleshooting host migrations](#).

Failed: The migration job has finished and all hosts failed to migrate. See [Troubleshooting host migrations](#).

Migration queue actions

In the migration queue, several actions are available to perform on one or more migration jobs.

Note: Click the migration job name link to open a specific migration job and make additional modifications or perform actions on one or more hosts in the job. See [Managing a host migration job](#).

For each migration job, these actions are available from the actions  menu:

- Open job details panel: The job details panel includes job overview info, such as the number of hosts currently assigned each migration status.
- Open job details page: Open the migration job to make modifications or perform actions on one or more hosts.
- Rename job: Change the name of the migration job.
- Start migration: If a migration job was created and the Assign to static host groups before migration option was selected, it appears in a Created state so you can assign static host groups in the destination CID. After assigning static host groups, click Start migration.
- Delete migration: You can delete a migration job that hasn't started and has a status of Created.
- Cancel migration: You can cancel a migration job that has started and has a status of Active. This action cancels the migration only for hosts that haven't finished migrating. If hosts in the job have finished migrating, their status is Completed and their migration can't be canceled.
- Export results: You can export the results in CSV or JSON format of a finished migration with a status of Completed, Failed, or Partially Failed.

These actions are available when you select one or more migration jobs:

- Delete open migrations: You can only delete selected migration jobs that haven't started and have a status of Created. If you select migration jobs that have started or finished, they aren't deleted.
- Cancel ongoing migrations: You can only cancel selected migration jobs that have started and have a status of Active. If you select migration jobs that haven't started or have finished, they aren't canceled. For each selected job with a status of Active, this action cancels the migration only for hosts that haven't finished migrating.
- Export completed results: You can export the results of finished migration jobs with a status of Completed, Failed, or Partially Failed. If you select a migration job that isn't finished, the results aren't exported.

Falcon Management

Managing a host migration job

After a migration job is created, you can manage it from the host migration details page, [Host setup and management > Manage endpoints > Host management](#) , then click [Host migration queue](#) and click the job name.

Host migration status

Each host on the migration job details page is displayed with one of these statuses after the migration job has started. If the migration job has a status of [Created](#) but hasn't started, the hosts are not displayed with a migration status.

- **Queued:** The host is queued for migration but hasn't started migrating
- **Running:** The host is currently migrating
- **Completed:** The host has been successfully migrated
- **Canceled:** The migration job has been manually canceled before the host was successfully migrated

Failed: The host was unable to be migrated and remains in the original CID. For more info about reasons migration for a host fails, see [Troubleshooting host migrations](#).

Host migration job actions

On the host migration details page, several actions are available to perform on the migration job or one or more hosts in the job.

These migration job actions are available:

- **Start migration:** If a migration job was created and the [Assign to static host groups before migration](#) option was selected, it appears in a [Created](#) state so you can assign static host groups in the destination CID. After assigning static host groups, click [Start migration](#).
- **Rename job:** Click [Actions > Rename job](#) to change the name of the migration job.
- **Delete migration:** Click [Actions > Delete migration](#) to delete a migration job that hasn't started and has a status of [Created](#).
- **Cancel migration:** Click [Actions > Cancel migration](#) to cancel a migration job that has started and has a status of [Active](#). This action cancels the migration only for hosts that haven't finished migrating. If hosts in the job have finished migrating, their status is [Completed](#) and their migration can't be canceled.

For each host in the migration job, these actions are available from the actions  menu:

- **Open details panel:** View migration details about the host, such as host status and a timeline of migration events.
- **Assign static host groups:** You can assign static host groups in the destination CID to the host if the job hasn't started and has a status of [Created](#).
- **Remove static host groups:** You can remove static host groups assigned to the host if the job hasn't started and has a status of [Created](#).
- **Remove from job:** You can remove the host from the migration job if the job hasn't started and has a status of [Created](#).

These actions are available when you select one or more hosts:

- **Assign static host groups:** You can assign static host groups in the destination CID to the selected hosts if the job hasn't started and has a status of [Created](#).
- **Remove static host groups:** You can remove static host groups assigned to the selected hosts if the job hasn't started and has a status of [Created](#). This option is only available when you select hosts that are assigned the same static host groups.

Remove from job: You can remove the selected hosts from the migration job if the job hasn't started and has a status of [Created](#).

Troubleshooting host migrations

When a host can't be migrated, its migration status is set to [Failed](#) in the migration job and the host remains in the original CID.

Migration for a host fails in these circumstances:

- If a host doesn't meet these requirements for migration, its migration status is immediately set to [Failed](#):
 - The host is not on a platform host migration supports. Only Windows, Mac, and Linux hosts can be migrated.
 - The host's sensor was installed using [DaemonSet](#) deployment.
 - The host is running a Falcon sensor version earlier than version 7.16.
 - The host is currently being migrated by another migration job.
- If the host is not accessible by the migration job due to one of these states, the migration job waits up to 45 days after the job was started for the host's state to change before setting the migration status to [Failed](#):
 - The host is network contained
 - The host is not online
 - The host is in reduced functionality mode (RFM)

Cloned host in destination CID for failed migrations

When a migration job runs, each host is cloned in the destination CID as part of its migration. If the migration fails for a host, it remains in the original CID and the incomplete, cloned host record remains in the destination CID. This cloned host remains and is inactive because it doesn't have an associated sensor connecting to the CrowdStrike cloud. Cloned hosts are automatically removed from the Falcon console according to the default retention of 45 days of inactivity, or you can manually hide or delete them after the migration job as part of [troubleshooting failed migrations](#).

Falcon Management

Managing scheduled reports

As a Flight Control customer, you can create and manage Scheduled reports ([Dashboards and reports > Dashboards > Scheduled reporting](#)) from both your parent and child CIDs. For more info, see [Scheduled Reports](#). Keep these additional benefits and limitations in mind as you manage your scheduled reports from the parent CID.

- The Scheduled reports index displays an aggregated list of scheduled reports created in your parent and child CIDs.
- An additional Customer column in the table shows the name of the CID that created the report. Customer names are searchable in the Scheduled reports index. You can use this column to identify which scheduled reports belong to which CIDs.
- You cannot edit scheduled reports created in a child CID from the parent CID, even if they're created by you. Switch your account view to a specific child CID to edit its scheduled reports.
- You can perform the following actions on child CID scheduled reports from the parent CID: Download current report, View report history, Take ownership, Run report, Deactivate, and Delete

Managing users

There are two types of users in Flight Control and multi-CID accounts: parent CID users and child CID users. In addition to the roles they are assigned, the access that a user has is defined by the CID they are created in.

- Users who are created in the parent CID have access to all child CIDs with the roles they've been assigned in the parent CID
- Users who are created in a child CIDs only have access to the specific child CIDs they've been created in

All default roles that are currently available can be assigned to users both at the parent CID and child CID levels.

Note: Custom roles must be created and assigned to users in their home CID. See [Managing custom roles](#).

For info about general user management, see [User Management](#).

Parent CID users

From the [User Management](#) page (Host setup and management > Falcon users > User management), you can add users to your parent CID. When you're managing users in the parent CID, you're managing users that have access to all child CIDs. When these parent CID users switch to different child CIDs, they assume the same roles they have in the parent CID.

For example, if a user has the Falcon Admin role in the parent CID, they'll have the same Falcon Admin access in all child CIDs.

Child CID users

To add users to a child CID, switch to the child CID, then add users from the [User Management](#) (Host setup and management > Falcon users > User management) page. Child CID users only have access to the specific CIDs they've been added to.

As a parent CID user, when you switch to a child CID to manage users, you're only managing users for the specific CID that you're in. Switch between child CIDs to manage their respective users.

Managing workflows

You can create and manage Falcon Fusion SOAR workflows in Flight Control environments. Rather than manage workflows for each CID individually, you can manage workflows in a parent CID and then apply them to one or more of its child CIDs.

For more info, see [Fusion SOAR](#).

Visualizing your Flight Control environment

Go to [Host setup and management > Flight Control management > CID overview](#) for an overview of your Flight Control environment. Get an overall picture of your multi-tenant architecture and CID-specific metrics in an interactive graph or table view.

Use the CID overview page to complete these tasks:

- Visualize the full Flight Control hierarchy at a glance
- Explore relationships between child and parent CIDs
- Understand how policy and detection data flow between CIDs
- View details about each CID
- Export and download the graph layout or selected table data to your local system

CID overview page considerations:

- The CID overview page shows only the CIDs you have access to.
- The Graph tab is available only for environments with fewer than 200 CIDs.
- The Table tab opens by default for environments with more than 50 child CIDs.

Review your CID hierarchy

Use Graph view

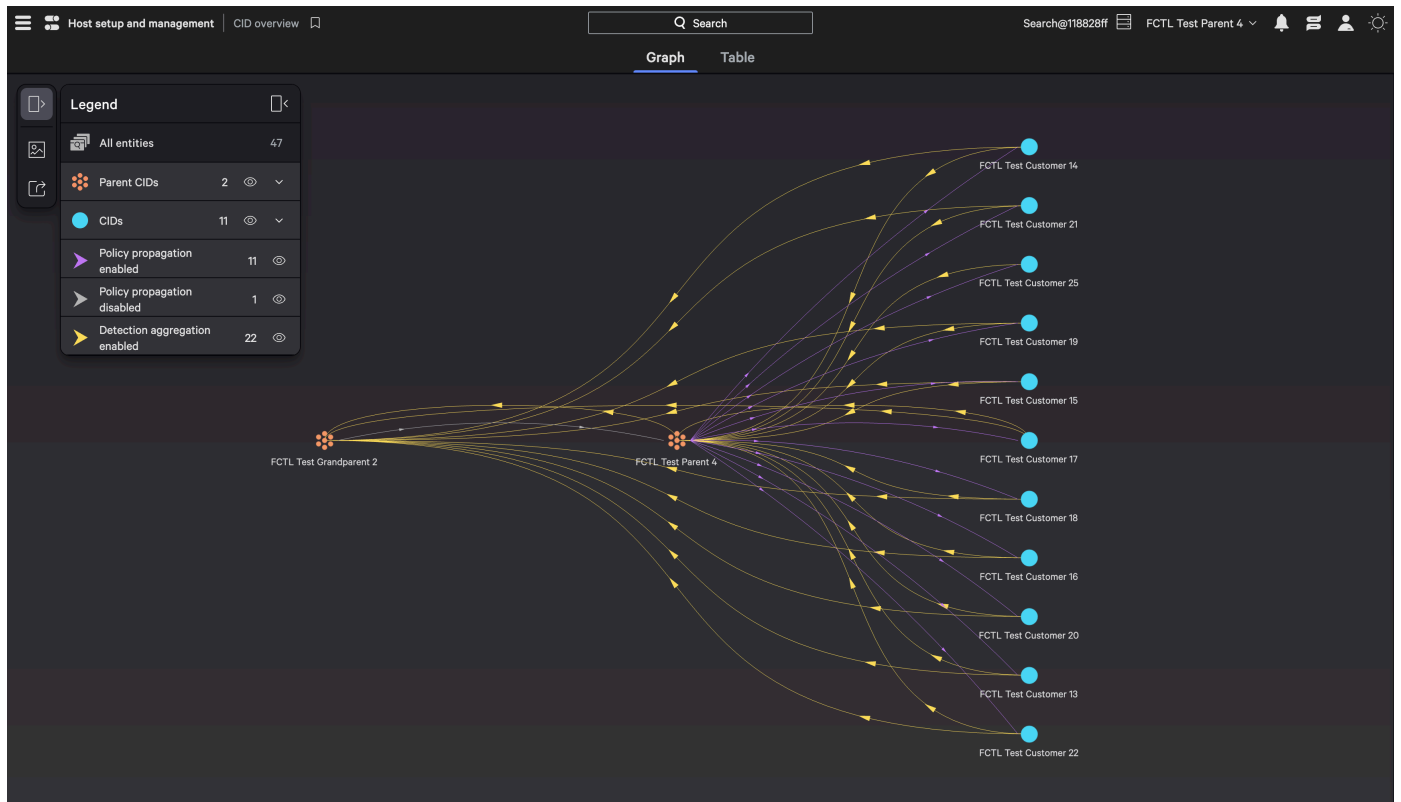
The Graph tab on the CID overview page visually models your Flight Control environment in a hierarchical tree graph. Nodes in the graph represent CIDs and directional lines map connections between them.

Note: The Graph tab is available only for environments with fewer than 200 CIDs.

You can interact with the graph and adjust the view to better understand the relationships between CIDs and inspect specific details.

Falcon Management

- Understand the hierarchical structure. Clearly see parent CIDs and the child CIDs that are connected to them.
- Understand data flow between CIDs. Arrows from parent to child CIDs indicate policy propagation flow. Arrows from child to parent CIDs show detection aggregation. You can hover over an arrow to view the description or click to highlight it.
- See basic CID info. Hover over a node to see info about the CID including assigned CID groups, CrowdScore, and detection and endpoint data.
- Show or hide the legend. Click the  Toggle legend icon to show or hide a legend explaining the entities, icons, and colors used in the graph. In the legend, expand the CID categories to see individual parent and child CIDs. You can then select a CID to open a panel with its details. You can also click the Hide icon to remove that type of entity from the graph view.
- Adjust the graph view. Click and drag to move the graph around the window. You can also scroll with your mouse to zoom.



View CID details

Click a node in the graph or select a CID on the legend to open a panel with more details about it, including Falcon modules and allowed domains. Switch between the Graph and Table tabs to view additional details for a selected CID.

Export and download

- Click the Download PNG icon to download an image of the current graph view in PNG format.
- Click the Export icon to generate and download a CSV or JSON file with your CID data selection in the Table tab, including each CID's Falcon modules, allowed domains, and CID groups.

Note: To download data for your entire Flight Control environment, go to the Table tab and click Clear All to remove any search parameters or filters before exporting.

Use Table view

The Table tab on the CID overview page arranges your Flight Control environment in a hierarchical table, with rows for CIDs and corresponding columns with details for each CID.

Note: The CID overview page opens the Table tab by default for environments with more than 50 child CIDs.

Complete the following tasks in the Table tab:

- View your CID hierarchy in a table with details for each CID. Child CIDs appear in alphabetical order below their parent CIDs.
- Customize your view by selecting the number of items displayed per page (20, 50, 100, 200). Click the  and  arrows to navigate between pages in your table.
- Search across your environment by entering a CID name or CID string.
- Filter your environment by Parent CIDs or Child CIDs. Click Clear All to reset your search and filter selections.
- See basic info about each CID by hovering over table cells. Click  Copy in the displayed dialog to copy the info to your clipboard.

Falcon Management

Host setup and managementCID overview

Search

Search@7ec4/706FCTL Test Grandparent 2

GraphTable

CID overview13 items

Search by CID name or CID stringCID typeClear all

Export

Details

CID name	CID type	CID string	Customer ID (check...)	Total child CIDs	Parent CIDs	Policy propagation to child CIDs	Detection aggregation from child CIDs	
FCTL Test Parent 4	Parent	aebbc77830b149cd...	AEBBC77830...	11	FCTL Test Gr...	Enabled	Enabled	
FCTL Test Grandparent 2	Parent	2f211c2291eb466c95b013b6b355b5e2	2F211C2291E...	11	--	Enabled	Enabled	
FCTL Test Customer 25	Child	a13d27451e3a4543...	AT3D27451E3...		FCTL Test Parent 4	Policy propagation from parent	Detection aggregation to parent	
FCTL Test Customer 22	Child	19040dc51e944de...	19040DC51E...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 21	Child	e64f0f6746264278...	E64F0F6746...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 20	Child	5273863dc3624398...	5273863DC3...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 18	Child	5efe2646b0924214...	5EFE2646B0...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 16	Child	5d882c791bd44c5e...	5D882C791B...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 13	Child	47e9c48f5a044c91...	47E9C48F5A...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 19	Child	9e2b763474da495...	9E2B763474...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 17	Child	6ee689adae7343ec...	6EE689ADA...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 15	Child	888298062d2a468...	888298062D...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	
FCTL Test Customer 14	Child	f323c9724984869...	F323C9724...		FCTL Test Grandparent 2, FCTL ...	Enabled	Enabled	

13 results (1-13 shown)Items per page50Page 1 of 1

FCTL Test Grandparent 2

CID details

CID string2f211c2291eb466c95b013b6b355b5e2

Customer ID checksum (CCID)2f211c2291eb466c95b013b6b355b5e2-97

Parent CIDs--Total child CIDs11

Detections on parent CID2,034Total detections across CIDs24,055Endpoints on parent CID24

Total endpoints across CIDs288Crowdcore

Falcon modules

Falcon PreventFalcon Host

No application and plugin integrations

Domains allowed

cloudstrike.com

Data flow

Detection aggregation from child CIDsEnabledPolicy propagation to child CIDsDisabled

View CID details

Click the  menu in a row and select Open details panel to open the CID details panel which includes additional info about a CID's Falcon modules, application and plugin integrations, and allowed domains.

View a CID in the Graph tab

Click the  menu in a row and select View on graph to view the CID's hierarchy and details in the Graph tab.

Note: The Graph tab is only available for environments with fewer than 200 CIDs.

Export and download data

Note: To download data for your entire Flight Control environment, click Clear All to remove any search parameters or filters before exporting.

Click  Export to generate and download a CSV or JSON file with CID data currently in the Table tab, including each CID's Falcon modules, application and plugin integrations, and allowed domains. Files are available for download for up to 24 hours after they are generated.

Flight Control access management

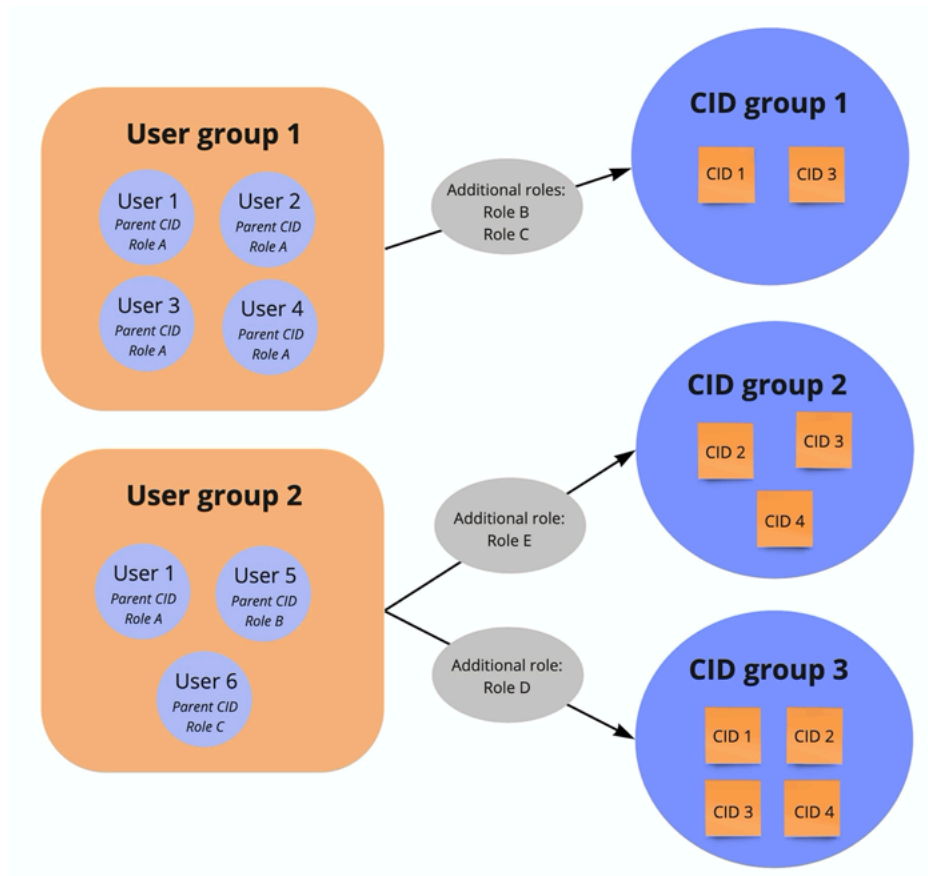
Flight Control access management gives you flexible, precise control over which child CIDs your parent-level users can interact with. With this feature, you define custom levels of access to certain child CIDs through a mapping of CID groups, user groups, and roles.

Understanding access management

Access management uses a group-based approach to facilitate flexible and simple regulation of user access across child CIDs in your environment. It's defined around relationships between CID groups, user groups, and their associated roles and permissions. Together, these components form a path for users to access child CIDs.

- CID group: A CID group organizes a subset of child CIDs into logical groupings. CID groups make child CIDs accessible to users in associated user groups.
- User group: A user group is a collection of users with similar access needs. User groups identify parent-level users who are given access to child CIDs in associated CID groups.
- Role: Users retain their assigned parent CID roles in user groups. Additional roles can be assigned to CID group/user group associations to grant permissions beyond each user's parent CID roles.

You manage access by forming user groups and CID groups and associating them with one another. Users are able to access the child CIDs defined in the associated CID group with their current parent CID roles. You can assign these associations additional roles to refine the level of access for all users in the user group. These roles are supplemental to each user's parent CID roles. When accessing a child CID, a user's level of access is determined by their assigned parent CID roles and any additional roles assigned to the group. For example, if a user's parent CID role is Falcon Analyst and they're given the Falcon Admin role through group assignment, they can access resources and perform actions allowed by both roles in associated child CIDs.



You can configure and affiliate multiple user and CID groups to meet the functional or security requirements of your organization. Individual child CIDs and users can belong to multiple groups, and a CID group or user group can contain up to 500 members. Access management's grouping mechanism streamlines scalable reuse of your CID groups and user groups for quick and easy application in a variety of contexts. You can create and associate groups based on categories or other logical groupings that fit your organization's needs (such as job function, department, or geographic location) and assign roles to those groups to access specific resources and complete tasks. For example, you might create a midwest device management user group and assign the Device Control Manager role to allow users to view Device Control dashboards and change Device Control policies in a group of midwest-based child CIDs.

After you create a CID group or user group, you can modify its name, description, members, and assigned roles.

Usage notes:

- Flight Control access management can only be applied to users in your parent CID.
- Careful consideration should be given when assigning parent CID roles to users. Roles assigned at the parent level stay with the user and cannot be excluded through user groups and CID groups.

Default CID group

Your parent CID comes with a predefined *Default* CID group that gives all parent-level users direct access to any child CID in the group in their parent CID role. By default, the *Default* CID group includes all child CIDs in your environment. If you want to limit user access to a specific child CID, you must remove the child CID from the *Default* CID group and add it to a new CID group with an assigned user group.

A child CID can belong to the *Default* group and custom CID groups at the same time. This gives all users parent-role access to the child CID while granting users associated with the custom CID group the additional access privileges defined by the group.

Access management group limits

When creating CID groups and user groups, note the following limits:

- Maximum 500 user groups per-environment
- Maximum 500 CID groups per-environment
- Maximum 500 users per user group
- Maximum 500 child CIDs per CID group

Known issues

Due to the way Falcon stores and processes data, any users in a parent CID who can view event data or LogScale dashboards in the Falcon console have access to data for all child CIDs.

To limit users' access to specific child CIDs, we've introduced two new user roles. Assign users one of these roles in the parent CID, then more specific roles in one or more child CIDs.

Falcon Management

- **Flight Control Managed Analyst:** Can access all areas of Falcon that support Flight Control CID group access restrictions, but not other areas of Falcon. It's available only with a Falcon Flight Control subscription.
- **Falcon Console Guest:** Can sign in to the Falcon console and view only profile, news, CrowdStrike Customer Center articles, and Falcon documentation. To grant additional access, add other roles to the same user. This role is available for all Falcon subscriptions.

Using access management

As a user with the Falcon Administrator role, you can create and manage CID groups and user groups to set up varying levels of user access to child CIDs in your environment.

Managing CID groups

Accessing CID groups

The CID groups page (Host setup and management > Flight Control management > CID groups) alphabetically lists the CID groups in your environment and includes high-level details and various actions that can be performed.

- a. View the total CID group count in your environment.
- b. Click Create CID group to open the new CID group workflow.
- c. CID group name: The name of the CID group.
- d. CIDs assigned: The child CID names assigned to the CID group.
- e. User groups assigned: The names of any user groups the CID group is assigned to. Note: "No user groups assigned" displays on the Default CID group. This CID group contains all users from your parent CID and user membership cannot be modified.
- f. Click the three-dot menu to access options for viewing, editing, or deleting a CID group.
- g. A set of dots displays on assigned CID and user group lists that do not fit in the view. Hover over the names that appear to view the full list of assignees.



Flight Control

> CID groups

Q Search

ABC Co Parent CID

CID Groups (8)

Create CID group

CID group name	CIDs assigned	User groups assigned	
Atlantic Region	Child A-3, Child A-12, Child A-26, Child B-16, Child B-19, C...	Device Managers, Admins	View CID group details Edit CID group Delete CID group
Default	Child A-2, Child A-4, Child A-6	No user groups assigned	
Enterprise Accounts	Child A-2, Child A-20, Child A-29, Child B-6, Child B-7, Chi...	Detections, Device Managers, Admins, Analysts	
New England Region	Child A-3, Child A-8, Child A-9, Child A-10	RTR, Device Managers, Admins	
Onboarding/New Accounts	Child A-30	RTR (read only)	
Pacific Northwest Group	Child A-17, Child B-15, Child D-11, Child D-23	RTR, Device Managers, Analysts, Detections, Read Only Analyst	
Small Business CIDs	Child A-11, Child A-12, Child B-9, Child C-3, Child D-10	Analysts	
Southwest Group	Child A-18, Child A-20, Child B-2, Child B-17, Child B-22, C...	Detections, Admins	

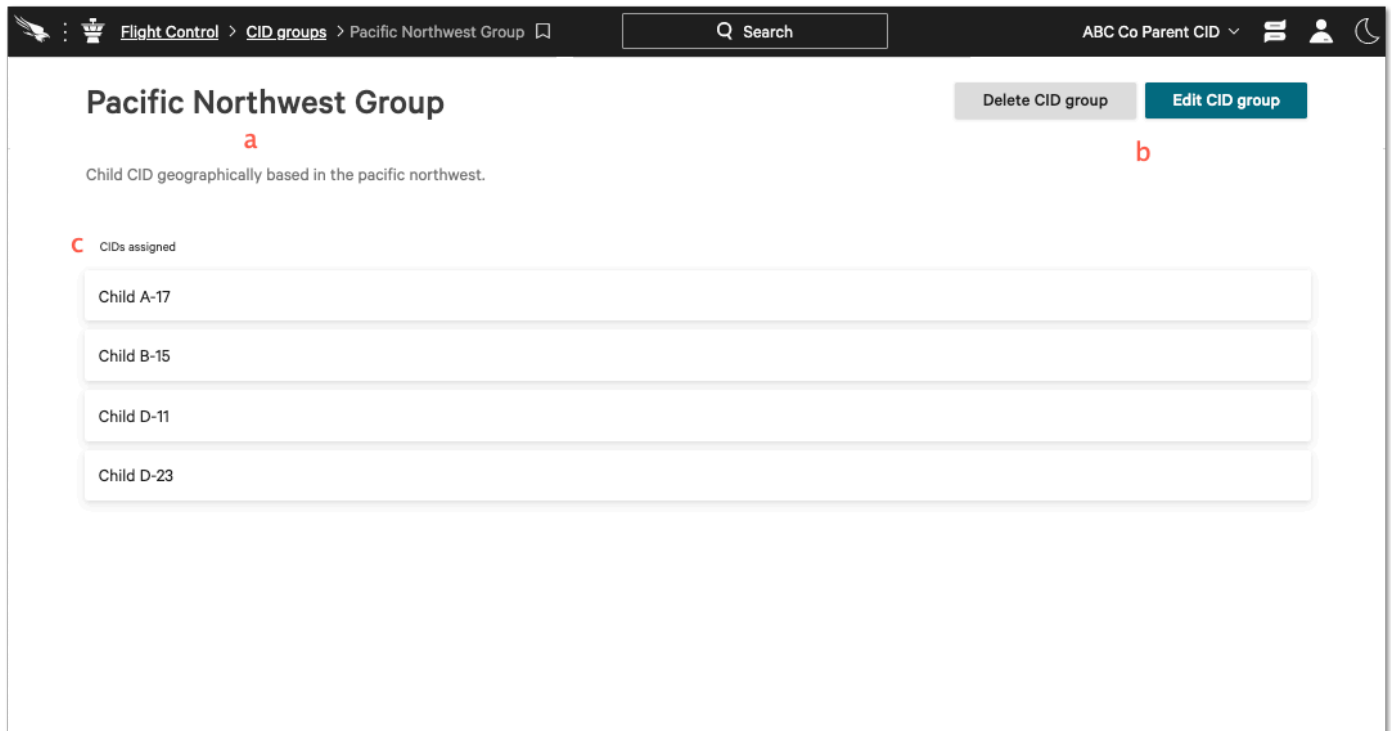
Falcon Management

Viewing CID group details

The CID group details page lets you view and manage the details of a CID group, including its name, description, and all of its assigned child CIDs. To access the user group details page, click

Open menu  then select View CID group details. For more info, see [Accessing CID groups](#).

1. View the CID group name and description (if one has been provided).
2. Options to Edit the CID group (name, description, and assigned child CID) or Delete the CID group.
3. CIDs assigned: Lists the names of child CIDs assigned to the CID group.



The screenshot shows the 'Pacific Northwest Group' details page. At the top, there's a navigation bar with 'Flight Control' > 'CID groups' > 'Pacific Northwest Group'. A search bar and user profile are on the right. The main header 'Pacific Northwest Group' has a red 'a' next to it. Below it is the description: 'Child CID geographically based in the pacific northwest.' To the right of the description is a red 'b'. On the right side, there are two buttons: 'Delete CID group' and 'Edit CID group'. Under the heading 'CIDs assigned' (with a red 'C'), there is a list of four child CIDs: 'Child A-17', 'Child B-15', 'Child D-11', and 'Child D-23', each in its own box.

Creating a CID group

Create a new CID group and add child CIDs to it. To create a CID group, enter a group name, provide an optional description, and select the child CIDs you want to include in the group. You can optionally create an empty CID group that does not have any child CIDs and add them later by [editing the group](#). After your CID group is created, grant access to select users by [assigning it to a user group](#).

1. Go to Host setup and management > Flight Control management > CID groups.
2. Click Create CID group in the upper right of the window.
3. Enter a name and optional description for the group in the fields provided. The name you enter displays on the CID groups page.
4. A list of your environment's child CIDs displays. Select the checkboxes of the child CIDs you want to add to the group. To add all child CIDs, check Select all.
5. Click Create CID group.

Editing a CID group

You can edit the name or description of an existing CID group. You can also add or remove child CIDs assigned to the group.

1. Go to Host setup and management > Flight Control management > CID groups.
2. Click Open menu  next to the CID group in the list and select Edit CID group. You can also open the CID group editor from the CID group details. For more info, see [Viewing CID group details](#).
3. Update the group name and description, as necessary. You can also select or deselect the checkboxes of child CIDs you want to add or remove from the group.
4. Click Update to save your changes.

Deleting a CID group

You can delete a CID group that you no longer need from the CID groups page. After a CID group is deleted, it's permanently removed from Falcon and cannot be restored.

1. Go to Host setup and management > Flight Control management > CID groups.
2. Click the three-dot menu on the right of the CID group you want to delete and select Delete CID group.
3. Click Delete in the confirmation window.

Falcon Management

Managing user groups

Accessing user groups

The User groups page (Host setup and management > CID management > Falcon user groups) lists all of the user groups in your environment in alphanumeric order. It also provides high-level details about each user group and various actions that can be performed.

- a. The numeric user group count displays at the top of the page.
- b. Initiate the workflow for creating a new CID group or user group.
- c. User group name: The user-defined name of the user group.
- d. Users assigned: The number of users assigned to the group.
- e. CID groups assigned: The names of the CID groups assigned to the user group.
- f. Click the three-dot menu to access options for viewing, editing, or deleting a user group.
- g. A set of dots displays on assigned CID group lists that do not fit in the view. Hover over the names that appear to view the full list of assignees.

The screenshot shows the 'User groups (7)' page in Falcon Management. At the top, there are buttons for 'Create CID group' and 'Create user group'. The table below lists the user groups with their respective user counts and assigned CID groups. A dropdown menu is open for the 'Read Only Analyst' group, showing options to 'View user group', 'Edit user group', and 'Delete user group'. The table data is as follows:

User group name	Users assigned	CID groups assigned
Admins	2	Enterprise Accounts, Southwest Group, Atlantic Region, New England Reg...
Analysts	2	Pacific Northwest Group, Enterprise Accounts, Small Business (
Detections	3	Southwest Group, Enterprise Accounts, Pacific Northwest Group
Device Managers	1	Pacific Northwest Group, Enterprise Accounts, New England Region, Atlan...
Read Only Analyst	2	Pacific Northwest Group, Southwest Group, Atlantic Region, New England Region
RTR	4	Pacific Northwest Group, Southwest Group, Atlantic Region, New England ...
RTR (read only)	1	Onboarding/New Accounts

Viewing user group details

The user group details page lets you visualize and manage the details of a user group, including all of its assigned users and CID groups. To access the user group details page, click Open menu then select View user group. For more info, see [Accessing user groups](#). User group information is broken into two sections: **Users** and **CID groups**. On the user group details page, you can view the user group name and description, if there is one. You can also find options to Edit the user group name and description or Delete the user group.

Users tab

- a. The Users tab shows a numeric count of how many users have been assigned to the group and lets you view high-level information about each assigned user.
- b. Click Assign users to add additional users from the parent CID to the user group.
- c. User email: The email address of the user provided in their parent CID user profile.
- d. User name: The name of the user provided in their parent CID user profile.
- e. Roles assigned: Any roles assigned to the user in their parent CID user profile.
- f. Click Remove on the right of a user in the list to delete the person from the user group.

Analysts

Users who are assigned the Falcon Analyst role.

a
Users (4) CID groups (3)

b
Assign users

c User email	d User name	e Roles assigned	f
alibrowne@email.com	Alison Browne	Falcon Analyst	Remove
tnguyen@email.com	Tony Nguyen	Falcon Analyst	Remove
cjames@email.com	Carly James	Falcon Analyst	Remove
kvang@email.com	Kevin Vang	Endpoint Manager, Falcon Analyst, Fa...	Remove

CID groups tab

- a. The CID groups tab displays a numeric count of how many CID groups have been assigned to the user group and lets you view high-level information about each assigned CID group.
- b. Click Assign CID group to add more CID groups to the user group.
- c. CID group name: The name of the CID group.
- d. Roles assigned: Any additional roles assigned to users in the group through the CID group/user group association.
- e. Click the three-dot menu to access options for editing the CID group roles or removing the CID group from the user group.

Analysts

Users who are assigned the Falcon Analyst role.

Users (4) **a** CID groups (3)

b **Assign CID group**

c CID group name	d Roles assigned	
Pacific Northwest Group	Falcon Analyst - Read Only	⋮
Enterprise Accounts	Falcon Analyst	⋮
Small Business CIDs	Falcon Analyst	e ⋮

Edit CID group
Remove CID group

Creating a user group

Create a user group and assign users to it. A user group can contain any number of users from your parent CID. You can create an empty user group that does not have any users and add them later. After your user group is created, [assign it to a CID group](#) to give the users access to the group's child CIDs.

1. Go to Host setup and management > Flight Control management > User groups.
2. Click Create user group in the upper right of the window.
3. Enter a name and optional description for the group in the fields provided. The name you enter displays on the [User groups](#) page.
4. Select the checkboxes of the users you want to add to the group. To add all users in your parent CID, check Select all.
5. Click Create user group.

Assigning a CID group to a user group

To apply access management, you must assign a CID group to a user group to form a relationship between them. You assign a CID group to a user group from the user group details. When connecting CID groups and user groups, you can apply roles to grant users additional permissions in the associated child CIDs.

1. Go to Host setup and management > Flight Control management > User groups.
2. Click the three-dot menu on the right of the user group in the list and select View user group.
3. Click the CID groups tab at the top of the page.
4. Click Assign CID group.
5. Click the Select CID group dropdown menu and choose the CID group name you want to assign to the user group from the list.
6. Optional. Select the checkboxes of any roles you want to apply to the group.
7. Click Save. The selected CID group and roles are applied to the user group.

Assigning users to a user group

Add new members to a user group from the User group details page. You can also assign a user to one or more user groups from within the User details. When you add a user to a user group, you give that person access and permissions granted through associated CID groups.

Adding members to a user group from the User group details page:

1. Go to Host setup and management > Flight Control management > User groups.

Falcon Management

2. Click the three-dot menu on the right of the user group in the list and select View user group.
3. Click Assign users.
4. Select the checkboxes of the users you want to add to the group.
5. Click Assign. The selected users are assigned to the group and appear in the user list on the user group details page.

Assigning a user to a user group from the User details:

1. Go to Host setup and management > Falcon Users > User Management and select View user details from the three-dot menu on the right of the user's name.
2. On the User details page, click the User Groups tab.
3. Click Assign user group.
4. In the Assign user groups window, select the checkboxes of the user groups you want to add the user to.
5. Click Assign. The selected user groups appear in the user's assigned user groups.

Removing users from a user group

You can remove user group members from the User group details page. You can also open the User details and remove the user from any assigned groups. After a user is removed from a user group, they no longer have access and permissions granted through the user group's associated CID groups.

Removing user group members from the User group details page:

1. Go to Host setup and management > Flight Control management > User groups .
2. Click Open menu  next to the user group in the list and select View user group.
3. Click Remove on the right of the user you want to remove from the group.
4. Click Remove in the confirmation window.

Removing a user from assigned user groups on the User details page:

1. Go to Host setup and management > Falcon users > User management , click Open menu  next to the user's name and select View user details.
2. On the User details page, click the User groups tab.
3. Click Remove on the right of the user group you want to remove.
4. Click Remove user group in the confirmation window.

Removing CID groups from a user group

You can remove a CID group associated with a user group from the *CID groups* tab of the user group details page. After a CID group is removed from a user group, access to the CID group through its association with the user group will no longer be valid.

1. Go to Host setup and management > Flight Control management > User groups.
2. Click the CID groups tab near the top of the page.
3. Click the three-dot icon on the right of the CID group you want to remove and select Remove CID group.
4. Click Remove CID group in the confirmation window.

Modify additional roles assigned to an associated CID group and user group

You can add or remove additional roles assigned to an associated CID and user group pair from the CID groups tab of the user group details page.

1. Go to Host setup and management > Flight Control management > User groups.
2. Click the CID groups tab near the top of the page.
3. Click the three-dot icon on the right of the CID group in the list and select Edit CID group.
4. Select or deselect the roles you want to add or remove.
5. Click Save to record your changes. The updated roles display in the CID group's details under Roles assigned.

Editing a user group name and description

After you create a user group, you can edit the name and description from the user group details.

1. Go to Host setup and management > Flight Control management > User groups.
2. Click Open menu  next to the user group in the list and select Edit user group. You can also open the user group editor from the user group details.

Falcon Management

3. Make changes to the user group name and description, as necessary.
4. Click Update to save your changes.

Deleting a user group

You can delete a user group if it's no longer needed. Deleting a user group is permanent. When you delete a user group, all connections to CID groups through the user group are removed.

1. Go to Host setup and management > Flight Control management > User groups.
2. Click the three-dot menu on the right of the user group in the list and select Delete user group. (Note: You can also delete a user group from the user group details.)
3. Click Delete in the confirmation window.

Generating an Access grant report

Run an Access grant report to generate a downloadable CSV or JSON file with a range of data about your users and their access rights to your child CIDs. To run the report, click Export on the User groups page (Host setup and management > Flight Control management > User groups) and choose an output format (CSV or JSON). After your report is generated, the file will be available for download under the Export access grant report drop-down for 24 hours.

Report fields

The Access grant report is available in CSV and JSON formats. Both formats contain essentially the same data, but they are geared for different purposes. CSV format is designed for human consumption. It omits most system identifiers and includes only user-friendly readable names. JSON format is designed for programmatic use. It includes both user-friendly names and system identifiers.

The table below lists all of the fields found in the report, broken down by CSV and JSON format.

CSV fields	JSON fields	Description
Target Customer	target_customer_name	Friendly name of the child CID
–N/A–	target_customer_cid	The ID of the child CID
First Name	user_first_name	User's first name
Last Name	user_last_name	User's last name
–N/A–	user_uuid	User's unique system-generated ID
Email	user_email	Email address in the user's profile
Home Customer	user_home_customer_name	Friendly name of the CID that the user was created under
–N/A–	user_home_customer_cid	ID of the CID that the user was created under
Roles	roles	Roles granted to the user for use in the child CID
Grant Type	grant_type	direct, default_cid_group, or user_group *See descriptions below
Parent Roles	parent_roles_name	Roles granted to the user for use in the parent CID (parent and parent group grant types)
Group Roles	group_roles	Roles assigned to the user through this user and CID group (parent group grant type)
Parent Customer	parent_customer_name	Friendly name for the parent CID (parent and parent group grant types)
–N/A–	parent_customer_cid	System identifier for the parent CID (parent and parent group grant types)
CID Group	cid_group_name	Friendly name of associated CID group (Parent group grant type)

Falcon Management

CSV fields	JSON fields	Description
–N/A–	cid_group_id	System identifier of associated CID group (parent group grant type)
User Group	user_group_name	Friendly name of associated user group (parent group grant type)
–N/A–	user_group_id	System identifier of associated user group (parent group grant type)

*Available grant types:

- Direct: Roles assigned to the user in their home CID (configured under [Falcon Users > User Management](#)).
- Default CID group: Roles automatically granted to the user for child CIDs in the Default CID group
- User group: Roles granted to user through a combination of user and CID groups

To run an Access grant report, you must have an administrative role at the parent CID level for your Falcon subscription, such as Falcon Administrator or Falcon Intel Admin.

1. Click Export access grant report.
2. Choose the file format for your report (CSV or JSON).
3. When the report is ready, click Download. Your report will remain available under the drop-down for 24 hours.

[Flight Control](#) > Customer ID (CID)

ABC Co Parent CID

CIDs (34)

Create CID group

Export access grant report

CSV

JSON

Files for download
access_grant_report-2021-08-25T16:47:17Z.json
Ready. This file expires August 26 at 9:47 AM.

Download
Delete

CID	CID string value	Assigned to CID groups
Child A-1	051f9e9439af4d0aa980f00fa636e20f	Atlantic Region, Enterprise Accounts
Child A-2	6ad3bdc7a63b4b9aa499e1283cf518fc	Pacific Northwest Group, Enterprise Accounts
Child A-3	6f003434e5feba13b3d5653d56e3297f	New England Region
Child A-4	9a030c51a2074dc1b2bd9ff2fb8bb43f	Enterprise Accounts, New England Region, New Accounts
Child A-5	895497de69994eb195c79a2908df2a6c	Southwest Region
Child A-6	1ebada85e6ec49c4bd96e18736ce1d90	Small Business CIDs, Atlantic Region
Child A-7	0d152b96cd5b45e8a0ff0574d9f9ae86	Pacific Northwest Group, Enterprise Accounts
Child A-8	0bb60ca588b255e5a0c04b42fcdcbaba2	Midwest Region
Child A-9	919953e292334b6ab08e8af3047c0f37	Atlantic Region, New Accounts
Child A-10	3b7156bd90e8a6f5a36316720a457a50	Southwest Region, Small Business CIDs

Load more

Viewing the Flight Control audit log

In the Falcon console audit trail ([Audit logs > Audit logs > Falcon UI](#)), you can view a history of user and access management activity across your Flight Control environment, including what change occurred, in which CID, when, and by whom they were made.

1. Go to [Audit logs > Audit logs > Falcon UI](#) .

Falcon Management

2. On the Falcon console audit trail page, set the Service field to Flight Control.

- Use filters to refine the audit log results, such as by Action (the type of activity that occurred), Company (a specific CID), and Time range.
- Click a column header in the log to sort by that attribute.

Flight Control audit log events

The audit log records the following events for Falcon Flight Control. You can view complete event details in JSON from [Investigate > Search > Advanced event search](#) or with the Event Streams APIs.

Action	Description
Create CID Group	A new CID group was created.
Update CID Group	A CID group name or description was updated.
Delete CID Group	A CID group was deleted.
Add CID Group Member	A CID was added to a CID group.
Deleted CID Group Member	A CID was removed from a CID group.
Create User Group	A new user group was created.
Update User Group	A user group name or description was updated.
Delete User Group	A user group was deleted.
Add User Group Member	A user was added to a user group.
Delete User Group Member	A user was removed from a user group.
Add Role	An Add Role event is logged when: • A CID group is added to a user group with or without assigning roles.* • A role is assigned to an existing CID group-user group pair. *An empty Role ID list displays when you add a CID group to a user group without assigning any roles.
Deleted Role	A Deleted Role event is logged when: • Note: A CID group is deleted. The Role ID list displays empty when a CID group is deleted. • A role is deleted from a CID group-user group pair.
Add Member	A child CID was added to a parent CID.
Delete Members	A child CID was removed from a parent CID.
User Access Grant Report	A User access grant report was generated.

APIs

All available OAuth2 APIs are supported with Falcon Flight Control and multi-CID accounts. At the parent CID level, you can manage your parent CID level OAuth2 IDs and secrets instead of managing them at the child CID level. With the parent/child account hierarchy, you're able to get access tokens on behalf of child CIDs using the parent ID and secret, so you don't need to switch into each child CID to generate hundreds of OAuth2 IDs and secrets and rotate them as they expire.

API clients and keys are managed through the parent CID in [API Clients and Keys](#) (Support and resources > Resources and tools > API clients and keys).

Detection APIs

With our detection APIs, we allow the same access token to access all child CIDs, which aggregates detections search results through a single request. This only applies to detections.

Falcon Management

Restful APIs

Falcon Flight Control and multi-CID accounts support these Restful APIs:

- Detections APIs: Search, aggregate, filter, and update detections
- Asset management APIs: Search and filter assets
- Vulnerability management APIs: Search, filter, and get detailed information about vulnerabilities and evaluation logic
- Host APIs: Search, filter, find details, network contain, and delete hosts
- Host group APIs: Create, update, and delete host groups
- IOC management APIs: Create, update, and delete indicators of compromise (IOCs)
- Policy APIs: Create, update, clone, and delete prevention and sensor update policies
- Real Time Response APIs: Run commands remotely on hosts using RTR
- User management APIs: Add, update, and remove users and assign user roles

For more info about using our OAuth2 APIs, see [CrowdStrike OAuth2-based APIs](#).

Streaming APIs

The Streaming API collects detection summary and audit events across all CIDs into a single stream.

Falcon Data Replicator (FDR)

Falcon Flight Control and multi-CID accounts support Falcon Data Replicator (FDR) through these configuration options:

- Individual feeds, where each child CID gets its own Amazon S3 bucket
- Aggregated feed, where Falcon data is consolidated across all CIDs into the same S3 bucket, arranged into folders by child CID

Note: Each child CID must have a Falcon Data Replicator subscription.

For Flight Control accounts, the aggregated feed is often preferred. With this type of feed, when you apply a filter to the feed for the parent CID, the filter is also applied to all of its child CIDs.

For more info, see [Falcon Data Replicator](#).

Assets

Monitor assets in your environment, view all asset connections in the asset graph view, and manage asset criticality.

About Assets

Assets are physical or virtual hardware, external IP addresses, DNS domains, or cloud resources. Learn about asset types and protection options to understand where to find more info about monitoring assets and increasing security.

Understanding assets

In the Falcon platform, assets are any physical or virtual hardware, external IP addresses, DNS domains, or cloud resources. This can include anything from workstations and servers, to printers and routers, to mobile devices and smart appliances, to industrial machinery and medical monitors, to cloud VMs and containers, and more.

Asset protection

Different assets are protected differently. The Falcon sensor is the CrowdStrike agent that observes, detects, and prevents potentially malicious activity that is occurring on disk or in memory. Assets in cloud environments are monitored by Falcon Cloud Security scans to find IOMs, IOAs, and new and changed cloud assets. Similarly, Snapshot is an agentless solution for certain cloud assets.

For comprehensive CrowdStrike protection, install the sensor, register your cloud accounts, or enable Snapshot on every asset that supports it.

What you can do with your assets depends on factors such as whether they're cloud assets or whether they have the sensor installed. For example, on assets that are managed with the sensor, you can set up prevention and detection policies, remediate vulnerabilities and other risks, and track asset resource usage and security settings in the Falcon console.

For more info about what you can do with different types of assets, see [Asset tasks](#).

Asset views

Each asset has its own vast library of metadata that includes details about its make, model, location, resources, purpose, and so on. In the Falcon console, assets are grouped into different views based on this metadata. For this reason, the same assets often appear on different pages. For example, a cloud asset such as an AWS EC2 instance that has the sensor installed can appear on the Managed assets page and the Cloud assets page. It's the same asset, but it appears in multiple places because of its metadata.

The various asset views can help you focus your asset-related tasks. For example, if you want to manage Purdue levels for your IoT assets, you can go to the XIoT security IoT dashboards. The same assets might appear on other asset pages, but the IoT pages focus on IoT-specific assets and tasks.

Falcon Management

Asset tasks

Task	Documentation
Learn about new assets in your environment and gain visibility into assets that don't or can't have the Falcon sensor installed.	Internal Asset Discovery
Monitor cloud assets: resources that are deployed, stored, or running in the AWS, Azure, or Google Cloud cloud computing environment.	View your Cloud Assets
Install the Falcon sensor and expand sensor coverage.	Sensor Deployment and Maintenance
Monitor asset sensor status, manage host settings, and assign assets to host groups to manage their policies.	Host and Host Group Management
Monitor security, account activity, resource usage, and application installation and usage on assets.	Asset Management
Investigate your network perimeter to find known and unknown internet-exposed (external) assets and assess the vulnerabilities associated with them.	Falcon EASM
Monitor IoT assets in your industrial control system (ICS) and operational technology (OT) environment.	XIoT Security
Understand the relationships between assets in a network, including which account should own a specific asset's remediation and other management tasks based on how frequently they log in.	Asset Management: Asset Graph View Asset Graph for Cloud Assets
Proactively identify potential risks and close attack paths to critical assets.	Attack Path Analysis Cloud Attack Path Analysis

Asset Inventory

Create custom tables for customizable visibility into data about assets and cloud assets.

Overview

Create custom tables for customizable views of asset data from across your environment.

Home

Dashboards

All assets

System insights

+

All assets

Preset | Shared table

Saved filters

Hostname

IP address history

Manufacturer

OS version

Last seen

Asset management

Add/remove filters

Clear all

1299 total filtered

Export

	Hostname	IP address history	OS version	Manufacturer	Last seen	Asset management	Actions
☐	del llw 1900709_	2024 112	RHEL 7.5	CsFlows System Manufacturer Inc	Mar. 6, 2024 16:00:00	Managed	
☐	—	2024 112	undefined	VMware, Inc.	Mar. 1, 2024 05:00:00	Unmanaged	
☐	2024 112	2024 112	Windows 10	VMware, Inc.	Mar. 1, 2024 05:00:00	Managed	
☐	—	2024 112	undefined	VMware, Inc.	Mar. 1, 2024 05:00:00	Unmanaged	
☐	2024 112	2024 112	Windows 11	Parallels International GmbH.	Feb. 2, 2024 10:00:00	Managed	
☐	2024 112	2024 112	undefined	VMware, Inc.	Mar. 5, 2024 18:00:00	Unmanaged	

1,299 results (1-50 shown)

Items per page

50

Page 1 of 26

Use the preset tables to see preconfigured views of commonly useful data. To focus on specific details or to summarize unique combinations of info for your organization's needs, you can create your own custom tables. When you're done, you can keep a table private, or you can share it with other users in your organization.

Falcon Management

Requirements

- Subscriptions:
 - To view only basic data about managed assets, requires one or more of these subscriptions:
 - Falcon Insight XDR
 - Falcon Prevent
 - Falcon Next-Gen SIEM (a Falcon Insight XDR add-on)
 - To view all data about assets, requires one or more of these subscriptions:
 - Falcon Discover
 - Falcon Exposure Management
 - To view data about cloud assets, requires one or more of these subscriptions:
 - Falcon Cloud Security
 - Falcon Cloud Security with Containers
- Sensor: All supported sensor versions
- Default roles:
 - To view all tables and to create or edit private tables: All roles with access to the Falcon console
 - To share tables and edit shared tables:
 - Falcon Administrator
 - Exposure Management Manager
 - Dashboard Admin

Before you begin

To see data in Falcon’s custom tables, your organization must have the relevant subscription and you must have the required user roles. The subscriptions and user roles required depend on the data source of each table.

Understanding custom tables

A table is a particular view of data from your Falcon environment. Each table has one data source, which determines not only the data but also the columns and filters you can select for that table. Tables appear as tabs, and you can save multiple table tabs in tab groups to keep similar info together. High-level admins can also share the tables they create and edit shared tables.

Data sources for tables

Each table retrieves info from a single data source. This table lists the available data sources and their corresponding subscriptions.

Table 1. Data sources and corresponding subscriptions

Data source	Subscriptions
Assets: Assets that are found by the sensor or third parties	For basic data about managed assets: • Falcon Insight • Falcon Prevent For all data about managed, unmanaged, and unsupported assets: • Falcon Discover • Falcon Exposure Management
Cloud assets: Assets that are found by CSPM	• Falcon Cloud Security • Falcon Cloud Security with Containers

Important: Different data sources can't be combined into the same table.

Table types

There are multiple types of Falcon tables.

Preset: Preset tables are built into Falcon and can't be edited. All preset tables that are available to your subscriptions are visible to all users in your organization.

Private: A private table is one that you've made by duplicating an existing table or creating a new one. When you duplicate or create a table, it's private by default. Only you can see and edit your private tables. Other users can't see or edit them.

Shared: With certain roles, you can share your private tables to let other users in your organization with those roles see and edit them. These roles include the Falcon Administrator, Exposure Management Manager, and Dashboard Admin role. As with any Falcon data, users in other organizations can't see or edit your shared tables.

Setup

No setup required. Custom tables are available to all Falcon users.

Falcon Management

View all assets

You can access all assets in your environment through the following navigation paths:

- [Asset inventory](#) > [Asset overview](#) > [All assets](#)
- [Next-Gen SIEM](#) > [Entity management](#) > [Hosts](#)

Manage custom tables

You can use Falcon's preset tables, customize an existing table, or create a whole new table.

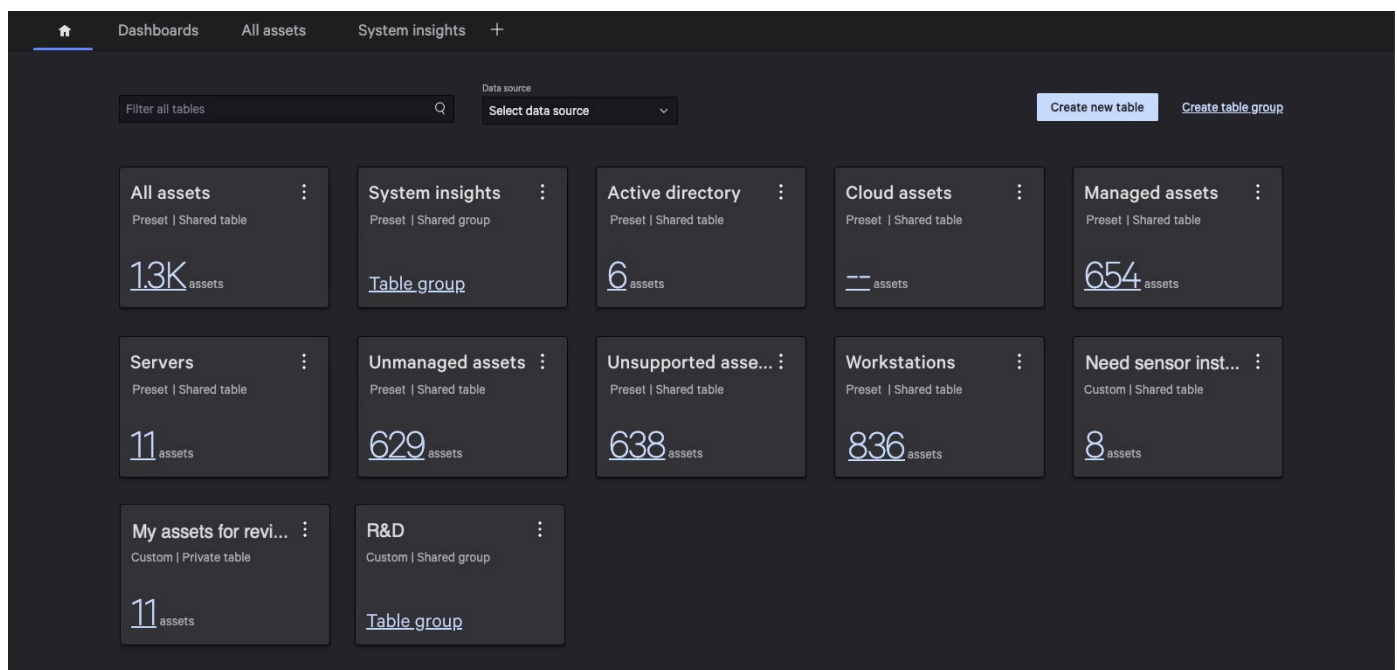
View tables

For customized tables about assets, go to [Asset inventory](#) > [Asset overview](#) > [Home](#) .

Depending on your subscriptions, you might have a [Dashboards](#) tab with dashboards of info about assets and cloud assets.

On the Home 🏠 tab, you can see all of your asset tables, including shared tables and any private tables you've created.

- Open a table: Click its tab or tile.
- Narrow your view: Filter by the table name or data source.
- Pin favorites: Click Open menu ⋮ , and click [Pin table](#) or [Pin table group](#) to pin that table or group to the top of your Home 🏠 tab.



Add a table

There are 2 ways to add new tables:

- Duplicate a table: Choose this to get a quick start based on an existing table.
- Create a table: Choose this to start with a blank table and add the filters and columns yourself.

Duplicate a table

When you duplicate a table, you create a second instance of that table in your Falcon environment. A duplicated table includes all of its saved filters and export templates. For example, you might duplicate a preset table to create an editable version of it or duplicate a private table before sharing it.

Duplicate tables are managed independently of the original tables. In other words, if you edit the original table, it doesn't affect the duplicated table.

If you duplicate a shared table, your new table is private by default. You can choose to share your new table later.

Duplicate a table from the table itself or on the Home 🏠 tab:

1. Click Open menu ⋮ and select Duplicate.
2. Enter a name for the new table.
3. Click Create duplicate table.

After duplicating a table, you can edit its default columns and filters and share it with others in your organization.

Falcon Management

Create a table

When you create a table from scratch, you determine the data source and which columns and filters are available by default. If you share the table with someone who duplicates it, any changes they make to the duplicate table don't affect your original table.

1. On the Home  tab, click Create new table.
 2. Select a data source. The data source you select determines which data, columns, and filters are available on your custom table:
 - Assets: Managed, unmanaged, and unsupported assets from asset management (Falcon Discover)
 - Cloud assets: Cloud VMs or containers that can have the sensor installed from CSPM
- Note: The data sources available to you are based on your subscriptions. For more info, see [Requirements](#).
3. Enter a name for your table.
 4. Optional. To add this table to a table group, select the group from the Add to table group (optional) menu. For more info, see [Manage table groups](#).
 5. Select the filters and columns to appear by default for this table. After you create a table, the filters and columns you don't select here are still available through the Add/remove filters + and Configure table columns  menus.
 6. Optional. To avoid saving any filters that you applied while creating the table, clear the Lock filter values with table creation checkbox. For more info, see [Lock filter values](#).
 7. Optional. To share this table, select the Shared table checkbox. For more info, see [Share a table](#).
 8. Click Create table.

Lock filter values

You can lock filter values so your saved tables always filter by certain data. For example, you might want to save a table that is always filtered by Device type: Server so you have a quick view of all servers in your environment.

To lock filter values, select the filters and values you want to save when creating a table, and leave the Lock filter values with table creation checkbox checked. You can't change locked filters without editing the whole table.

Share a table

By default, your custom tables are private. You can choose to share them with others in your organization, but after a table is shared, you can't make it private again.

- Private: Only you can see and edit your private tables. Other users can't see or edit them.
- Shared: Other admin users in your organization can see, edit, and delete your shared tables. Users outside your organization can't see or edit them, as with all your Falcon info.

You must have the Falcon Administrator, Exposure Management Manager, or Dashboard Admin role to share tables.

Tip: Before sharing a table, consider duplicating it to keep a private backup copy. For example, admin users can delete shared tables, so you might want to keep a private copy.

Share a private table from the table itself or on the Home  tab:

1. Click Open menu  , and click Share.
2. Click Share table.

You can also share a table at the same time you create it. For more info, see [Create a table](#).

Edit a table

When you edit a table, you can add, remove, and rearrange its default columns and filters. You can edit only private and shared tables. You can't edit preset tables, but you can duplicate a preset table and edit the duplicate.

Note: You can't change a table's data source.

Edit a table from the table itself or from the Home  tab:

1. Click Open menu  and click Edit default settings.
2. Optional. Change the default filters and filter values.
3. Optional. Change the default columns.
4. Click Update table.

Rename a table from the table itself or from the Home  tab:

1. Click Open menu  and click Rename.
2. Enter a new name.
3. Click Rename table.

Delete a table

Deleting a table permanently removes it from the Falcon console. If a table is shared with your organization, it's deleted for all users. Deleted tables can't be recovered.

Deleting a table also deletes its saved filters.

Delete a table from the table itself or from the Home  tab:

1. Click Open menu  and click Delete.
2. When asked, click Delete to confirm.

Manage table groups

Group multiple tables to keep similar info together, keep your workflows moving smoothly, and prioritize important tables.

Note: Table groups can only include either private tables or shared tables, not both.

Create table groups

Create a table group from a table or from the Home  tab:

1. Click Open menu  and select Create new table group.
2. Enter a name for the table group.
3. Select the tables you want to be part of the group.
4. Click Create table group. The tables you added to the group appear in the new group tab as subtabs.

Add a table to a group

Add a table to an existing table group from the table or from the Home  tab:

1. Click Open menu  and click Add / remove tables.
2. Select the tables you want to add to the group.
3. Click Save and update table group.

Edit and delete table groups

You can duplicate, share, and rename table groups the same as individual tables. When you duplicate a table group, all tables in that group are duplicated, as well.

You can also either ungroup or delete a table group:

- Ungroup: Remove the grouping but retain all of the tables within the group.
- Delete: Delete the group and all tables within the group.

Export reports

Export any table as a report that you can share within your environment.

Quick exports

Export a CSV file of the info as you see it in the console, or export from a saved template.

1. Click Export.
2. Select a quick export option:
 - Choose CSV of current selection to export the table as a CSV file.
 - Choose a saved export template.

Configure exports

Configure exactly which data you want to see in an export.

1. Click Export.
2. Select New export or template.
3. Select CSV or JSON.
4. In the Available data section, select the columns you want to include in your exported report. By default, the Selected data section includes the data visible in the current table.
5. In the Selected data section, drag the data to reorder it in your export.
6. Click Export.

Download exported reports

View and download the 5 most recently run exports.

1. Click Export.
2. Select Completed exports. The Completed exports section shows the number of exported reports that are ready to download.

Falcon Management

3. Click Download  for the report you want. The export report downloads to your device's default downloads folder.

Configure export templates

Save an export as a template to reuse within your environment. Export templates are shared within an environment across users. Environments can have a maximum of 10 saved templates.

1. Click Export.
2. Select New export or template.
3. Click Save as template for future use to reuse the configuration as a template.
4. Enter a name.
5. Select CSV or JSON.
6. From the Available data section, choose the data you want to see in your export.
7. In the Selected data column, drag the columns to reorder them in your export. By default, the Selected data column includes the columns visible in the current table.
8. Click either Save and export or Save without exporting.

Edit export templates

Edit export templates to match your environment's needs.

1. Click Export.
2. Select Saved templates.
3. Click Edit  to edit a template.

Delete export templates

Delete export templates that no longer meet your environment's needs.

1. Click Export.
2. Select Saved templates.
3. Click Delete  to delete a template.

Asset Criticality

Assign asset criticality manually or dynamically with rules.

Asset criticality overview

In any environment, some assets are more critical to track than others simply because of the roles they play in the functioning and security of the network. For example, assets that are servers or are exposed to the internet are often more open to attack than other assets and require more tracking.

You can assign asset criticality to make it easier to find and prioritize such assets for threat mitigation and vulnerability remediation.

You can also see asset criticality assignments using APIs. For more info, see Asset Management APIs.

Requirements

- Subscriptions:
 - Falcon recommended rules:
 - Falcon Exposure Management (a Falcon Insight XDR add-on)
 - Assign criticality manually or with dynamic rules you create:
 - Falcon Insight XDR
 - Falcon Next-Gen SIEM (a Falcon Insight XDR add-on)
 - Falcon Discover (a Falcon Insight XDR add-on)
 - Falcon Exposure Management (a Falcon Insight XDR add-on)
- Sensor: All supported sensor versions
- Default roles:
 - Configure rules and assign asset criticality levels:
 - Falcon Administrator
 - Exposure Management Manager
 - Exposure Assets Admin
 - NG SIEM Administrator
 - NG SIEM Security Lead
 - View asset criticality levels and criticality rules:
 - Falcon Administrator
 - Exposure Management Manager
 - Exposure Assets Admin
 - Exposure Assets Analyst
 - Falcon Security Lead
 - Falcon Investigator
 - Falcon Analyst - Read Only
 - NG SIEM Administrator
 - NG SIEM Analyst - Read Only
 - NG SIEM Analyst
 - NG SIEM Security Lead
 - Event Viewer

Falcon Management

Understanding asset criticality

Asset criticality describes how important an asset is to your environment. In many cases, assets are either critical or not critical, with no ranking in between. However, most environments have some assets that are particularly important to prioritize for threat mitigation and vulnerability remediation. For this reason, you have 3 criticality levels for more flexibility in distinguishing among your assets, Noncritical, High, and Critical, as well as a default level before a criticality is assigned:

- Unassigned: All assets are unassigned until they're assigned a criticality level
- Noncritical: Most typical assets are noncritical
- High: Important assets such as servers or domain controllers
- Critical: The most important assets such as internet-exposed assets or a central server

Assign asset criticality to make it easier to find and prioritize such assets for protection against adversaries. Certain features, such as attack path analysis and risk-based vulnerability prioritization, depend on asset criticality.

For more info about these features, see [Attack Path Analysis](#) and [Risk-based vulnerability prioritization](#).

Understanding criticality assignment

You can assign asset criticality either manually or dynamically. Dynamic assignment is based on rules. Falcon recommended rules assign asset criticality levels based on security best practices and AI insights. You can also create rules that take precedence over the Falcon recommended rules. For more info, see [Understanding Falcon recommended rules](#).

You can dynamically assign criticality to managed assets only.

If you assign criticality manually or with rules that you create, you need to consider what criteria make an asset critical to your environment. For more info, see [Setup](#).

Understanding Falcon recommended rules

Falcon recommended rules require a Falcon Exposure Management subscription.

Because creating your own criticality rules from scratch can take time, we recommend rules to help keep your asset criticality assignments relevant and up to date. These Falcon recommended rules evolve based on security best practices and continuously emerging AI insights.

The AI insights are drawn from manual criticality assignments and dynamic criticality rules made across the CrowdStrike community to help ensure new Falcon recommended rules remain relevant and effective. This data is anonymized and aggregated to inform our AI model without directly linking the data to you.

Important: By using Falcon recommended rules, you give CrowdStrike permission to anonymize and aggregate the criticality rules you create to inform our AI model. You can opt out of sharing your criticality rules data by turning off Falcon recommended rules. For more info, see [Set up Falcon recommended rules](#).

In most cases, new Falcon recommended rules are automatically available and enabled in your environment. However, if you created custom criticality rules before we released the first Falcon recommended rules on January 27, 2025, then new Falcon recommended rules aren't automatically enabled. This approach lets you review and manually enable them as you prefer.

New Falcon recommended rules become available as the AI model processes new data. Because these rules are based on insights extracted from a crowdsourced model that is constantly maturing, we recommend reviewing these rules periodically to make sure they make sense for your environment.

Asset criticality terminology

- Asset: Any physical hardware, virtual hardware, or cloud asset in your environment:
 - Managed asset: An asset that has the Falcon sensor installed; also called a *host*
 - Unmanaged asset: An asset that can have the Falcon sensor installed but does not
 - Unsupported asset: An asset that can't have a Falcon sensor installed
- Asset criticality: The importance of an asset to your environment:
 - Unassigned: All assets are unassigned until they're assigned a criticality level
 - Noncritical: Most typical assets are noncritical
 - High: Important assets such as servers or domain controllers
 - Critical: The most important assets such as internet-exposed assets or a central server
- Asset role: The role the asset plays in your environment. For more info, see [Override asset roles](#). Asset roles are assigned automatically and are available only with a Falcon Exposure Management subscription.
- Internet exposure: Whether the asset is exposed to the internet, as determined either automatically with Falcon EASM or manually by a user override. For more info about Falcon EASM, see [Internet Exposure](#).

Data refreshing

Criticality levels usually begin to propagate across your environment within a few minutes of being assigned. In the meantime, other features that rely on the value, such as exported reports and attack paths, might show conflicting values.

Dynamic rule-based criticality: If an asset that meets your criteria connects to your environment, it is assigned a criticality level within a few hours of when its Falcon sensor connects to the cloud or the asset is first seen. Rules are reevaluated and reapplied several times a day to keep your info up to date.

Dynamic rule precedence: New rule precedence can take a few hours to propagate across all of your assets.

Falcon recommended rules: New rules become available as the AI model evolves rather than following any preset schedule. Falcon recommended rules are considered new for 7 days.

Falcon Management

Setup

Some setup is required for Falcon recommended rules. Some setup might be required depending on your Falcon recommended rules preferences. For more info, see [Set up Falcon recommended rules](#).

Complete setup is required for manual or custom rule-based criticality assignment. Before you assign criticality manually or with custom rules, you must consider what criteria make an asset critical to your environment. For more info, see [Set up criticality criteria](#).

Set up criticality criteria

Before you assign criticality levels, consider the criteria of assets that are critical to your environment. These are some of the criteria often considered:

- Entry points, such as internet-exposed assets
- Business criticality, such as domain controllers and critical IT systems
- High value, such as payment card servers and medical record servers

Using these guidelines or your own, note your criticality criteria. Then, either filter your asset tables by those criteria and manually assign criticality levels, or set up rules to dynamically assign criticality levels to assets that meet your criteria. For more info, see [Manually assign asset criticality levels](#) and [Dynamically assign asset criticality levels](#).

Note: For Linux servers and workstations to be distinguishable, network events must be enabled in Falcon sensor for Linux on all of your hosts. For more info, contact Support.

Set up Falcon recommended rules

Contributing your custom criticality rules to CrowdStrike's AI model improves asset criticality assignments for all CrowdStrike customers. When Falcon recommended rules are turned on, your custom rules are anonymized, aggregated, and stored for our AI model training.

You have control over your data contribution:

- To contribute your rules to the AI model and receive new Falcon recommended rules, leave this feature turned on.
- To opt out of contributing your rules and out of receiving new Falcon recommended rules, turn off the feature within 7 days of its being enabled on your CID.

Turn on Falcon recommended rules

In most cases, Falcon recommended rules are already available and automatically applied to your environment. If they're not, you can enable these settings.

Important: By using Falcon recommended rules, you give CrowdStrike permission to anonymize and aggregate the criticality rules you create to inform our AI model.

1. Go to [Exposure management > Setup > Asset criticality rules](#) .
2. Click [Configure recommended rule settings](#).
3. Configure your preferences:
 - [Falcon recommended rules: Enable to show new Falcon recommended rules as they become available](#). You can then review these rules individually to apply them or not based on your criteria.
 - [Apply Falcon recommended rules: Enable to automatically apply new Falcon recommended rules as soon as they're available in your environment](#).
4. Click [Confirm](#).

Turn off Falcon recommended rules

Turning off Falcon recommended rules has 2 effects. It prevents your data from contributing to our AI model, and it prevents new Falcon recommended rules from being available on the [Asset criticality rules](#) page.

Any of your data that already contributed to the AI model remains part of the model. Any Falcon recommended rules that were recommended while the Falcon recommended rules setting was enabled remain available after you turn it off.

1. Go to [Exposure management > Setup > Asset criticality rules](#) .
2. Click [Configure recommended rule settings](#).
3. Disable the [Falcon recommended rules](#) setting. This also automatically disables the [Apply Falcon recommended rules](#) setting.
4. Click [Confirm](#).

Manage asset criticality

Review your assets' criticality levels and audit any changes made to criticality assignments over time.

Assign asset criticality either manually or dynamically based on rules. Review [Falcon recommended rules](#) to determine whether they meet your criticality criteria, and create new rules to further focus your dynamic assignments.

Dynamic criticality rules don't apply to assets that are already manually assigned a criticality level. You can manually override any criticality levels, whether they were assigned manually or dynamically.

Review criticality assignments

The asset details panel and details page list information about criticality assignments:

- Criticality level
- Whether it was manually or dynamically assigned
- Whether a dynamic assignment was based on a Falcon recommended rule

For manual assignments, click [Manually assigned](#) to view more info and update the criticality.

For rule-based assignments, click [View rule](#) to open a new tab where you can view more info and explore the rule precedence. For more info, see [Dynamically assign asset criticality levels and Establishing rule precedence](#).

Changes made to asset criticality are available in [Audit logs](#) in the Falcon console.

Falcon Management

Find assets by criticality

Filter by Asset criticality in any assets table:

- Filter by Critical to find assets to prioritize for Falcon sensor and OS updates, remediating vulnerabilities, or ensuring domain controllers or unsanctioned servers aren't exposed to the internet.
- Filter by Unassigned to find assets with no criticality level assigned to determine which level they should have.

Manually assign asset criticality levels

You can assign the same asset criticality level to up to 100 assets at the same time from any assets table:

1. Filter by the criteria that you determined define the criticality level you're assigning.
2. Select the checkbox for one or more assets.
3. Click  Assign asset criticality.
4. Select a criticality level.
5. Optional. Enter a description.
6. Click Assign or Update criticality.

For a single asset, you can also assign or edit criticality through the menu in the Actions column or from the Actions menu on the asset's details panel or page.

1 of 2 selected

Select up to 100 items for bulk actions

Assign criticality

Clear

	Hostname ^	Asset ID	IP address	MAC address	Organization	Asset criticality	Platform	OS version	Last seen	Actions
	ABC-123-D...					Unassigned	Mac	Big Sur (11.0)	May 10, 2023	
	ZYX-987-W...					Unassigned	Mac	Monterey (1...	May 17, 2023	

Dynamically assign asset criticality levels

Criticality rules dynamically assign appropriate criticality levels to assets in your environment based on the criteria in the rules. If key details about current assets change or new assets join your network, these rules proactively assign criticality to those assets.

You can create criticality rules to dynamically assign appropriate criticality levels to assets in your environment based on criteria you determine. For more info, see [Set up criticality criteria](#). Rules you create based on your own criteria always take precedence over any Falcon recommended rules you have enabled.

When setting up criticality rules, consider how the order of your rules affects how they're applied. For more info, see [Establishing rule precedence](#).

Manage Falcon recommended criticality rules

Review new Falcon recommended rules at least every 7 days to determine whether they meet your criticality criteria. For more info, see [Find new Falcon recommended rules](#) and [View asset criticality rule criteria](#).

Falcon recommended rules can't be modified. If a rule doesn't quite apply to your environment, you can duplicate it and edit the copy. For more info, see [Duplicate an asset criticality rule](#) and [Edit an asset criticality rule](#).

If a rule doesn't apply to your environment at all, you can disable it. For more info, see [Disable an asset criticality rule](#).

Note: Falcon recommended rules are enabled by default if you hadn't already created any criticality rules in your environment before January 27, 2025. If you had already created criticality rules before January 27, 2025, then Falcon recommended rules are not enabled by default so you can review them before applying them.

You can also change the default behavior of Falcon recommended rules in your environment. For more info, see [Set up Falcon recommended rules](#).

Find new Falcon recommended rules

New rules become available as the AI model evolves. Falcon recommended rules are considered new for 7 days, so we recommend reviewing these rules weekly to make sure they're relevant for your environment.

1. Go to Exposure management > Setup > Asset criticality rules .
2. If a new rule is available, an info message appears on the page. Click View rule to review its criteria.

Create an asset criticality rule

1. In the Falcon console, go to the Asset criticality rules page:
 - For those with a Falcon Exposure Management subscription, go to Exposure management > Setup > Asset criticality rules .
 - For those with Next-Gen SIEM, go to Asset inventory > Asset overview > Asset criticality rules .
2. On the Asset criticality rules tab, click Create criticality rule.
3. In the Name field, enter a name for the rule.

Falcon Management

4. Select the criteria that define the assets and the installed applications that this rule applies to.

Note: Asset roles require a Falcon Exposure Management subscription. Installed applications criteria requires a Falcon Exposure Management or Falcon Discover subscription.

5. Select the criticality level this rule will assign to assets that meet the criteria.
6. Optional. Enter a rule description.
7. Click Create rule.

The rule you created appears in the Asset criticality rules table, where you can change the rule precedence. For more info, see [Change the precedence of asset criticality rules](#).

Each CID can have up to 100 asset criticality rules at the same time. Asset criticality rules that you make in one CID aren't available in other CIDs.

Asset criticality rules 98 items

Criticality rule ▾ Rule status ▾ Asset criticality level ▾ Company : 1 applied ✕ Add/remove filters + Clear all Edit precedence Create criticality rule

Last modified ▾

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361

1362

1363

1364

1365

1366

1367

1368

1369

1370

1371

1372

1373

1374

1375

1376

1377

1378

1379

1380

1381

1382

1383

1384

1385

1386

1387

1388

1389

1390

1391

1392

1393

1394

1395

1396

1397

1398

1399

1400

1401

1402

1403

1404

1405

1406

1407

1408

1409

1410

1411

1412

1413

1414

1415

1416

1417

1418

1419

1420

1421

1422

1423

1424

1425

1426

1427

1428

1

Falcon Management

2. In Open menu  in the Actions column, click Duplicate rule.
3. Make your changes and click Duplicate rule.

Important: You must make changes to duplicated rules before you save them. To avoid asset criticality assignment conflicts, multiple rules with the same filters and criticality level can't exist at the same time.

Edit an asset criticality rule

1. On the [Asset criticality rules](#) page, find the rule you want to edit.
2. In Open menu  in the Actions column, click Edit rule.
3. Make your changes and click Update rule.

Note: Falcon recommended rules can't be edited. See [Duplicate an asset criticality rule](#).

Disable an asset criticality rule

On the [Asset criticality rules](#) page, disable the toggle in the Rule status column.

See all assets a rule applies to

To see the assets that are affected by a rule, go to [Exposure management](#) > [Setup](#) > [Asset criticality rules](#) and look at the Estimated | Actual matches column for that rule:

- Estimated: Assets that meet the rule's criteria
- Actual matches: Assets whose criticality is assigned by the rule

The estimated and actual counts often don't match because not every asset that meets the rule's criteria gets assigned a criticality level by that rule. This mismatch is due to rule precedence. Rules with a higher precedence override rules with a lower precedence, so an asset might meet the criteria of a lower-precedence rule but have its criticality actually assigned by a higher-precedence rule. For more info, see [Establishing rule precedence](#).

Click the number of assets in the Estimated | Actual matches column to open the assets table filtered by those assets.

Delete an asset criticality rule

This permanently deletes the rule. Any assets assigned a criticality level using this rule are assigned a criticality level of Unassigned when the rule is deleted.

1. On the [Asset criticality rules](#) page, find the rule you want to delete.
2. In Open menu  in the Actions column, click Delete rule.
3. In the confirmation window, enter Delete and click Delete criticality rule.

Note: Falcon recommended rules can't be deleted. See [Disable an asset criticality rule](#).

Establishing rule precedence

Rule precedence determines which rule's configuration settings are applied when more than one rule is available. You define rules with different precedences so that the first rule that matches the criteria for an asset is applied.

On an asset, the rule with the highest ranking precedence (1 being highest) is applied and active. If that highest-ranking active rule gets disabled, deleted, or moved in the order of precedence, then the next highest-ranking rule is applied and becomes active. For this reason, you should arrange rules in order of most specific to most general.

Note: Manual criticality assignments override any dynamic assignments based on rules. All rules you create are applied before Falcon recommended rules.

Change the precedence of asset criticality rules

1. On the [Asset criticality rules](#) page, click Edit precedence.
2. Drag the rules up or down to rearrange them.
3. Click Save.

Note: It can take a few hours before the new precedence is applied across all of your assets.