Threat Control System Administrator's Guide 5.0.1

November, 2024

Table of Contents

Getting Started **6**

Overview 6

Intended Audience 6

System Requirements 7

Authentication 7

Logging using Organization's Keycloak 7

Logging using Single Sign On (SSO) 8

User Accounts **9**

User Types 9

Prerequisites 10

Administration Tasks **11**

Organization Info 12

Audit Trail 12

Searching Audit Record of a User 12

Feature Flag 13

Enabling Features 13

Notification Management 15

Adding Notifications 15

Open Search Management 17

Adding Policies 17

Viewing Indices 19

Session Management 19

Viewing Session Management 20

Cancelling a Session 20

Searching for a Session 20

Enabling Search Factors for User Sessions 21

Organization Management 21

Viewing Organizations 22

Searching for Organizations 23

Enabling Search Factors for Organizations 24

Adding Organizations 24

User Behavior Analytics 24

Viewing User Insights 25

User Management 27

Users 28

Adding Users 28

Editing a User 29

Blocking or Unblocking a User 30

Inactivating a User 30

Searching for a User 31

Enabling Search Factors for Users 31

User Groups 32

Adding User Groups 32

Searching for a User Group 33

Enabling Search Factors for User Groups 34

IDP Groups 34

Adding IDP Groups 35

Searching for an IDP Group 35

Enabling Search Factors for IDP Groups 36

Auth Users 36

Adding Auth Users 37

Service Account 38

Adding Service Accounts 38

Creating Access Token for APIs 39

Support to Add IP Blocklists to Network Devices 41

Prerequisites 42

Types of IP Block Lists and Their Usage 42

Configuring Security Devices 49

Viewing the Blocked IP Addresses 52

Creating Security Policies 54

API List 54

Appendix 57

Managing Users in Organization's Keycloak 57

Logging in to Keycloak 57

Adding a New User 58

Deleting the Existing Users 62

Configuring Okta IDP for SSO 62

Registering a New Application in Okta 63

Adding a New User and Setting the Authentication Policy 67

Integrating Okta with Threat Control System 71

Configuring Microsoft Azure IDP for SSO 72

Configuring Access Token for Single Sign On (SSO) 73

Creating an Application Role to Assign to Groups 74

Assigning a Group to the Application in Microsoft Azure 75

Getting Started

This section includes information on system requirements and how to log in to Threat Control System.

The following topics are covered:

Overview 6

Intended Audience 6

System Requirements 7

Authentication 7

Logging using Organization's Keycloak 7

Logging using Single Sign On (SSO) 8

Overview

Threat Control System is a threat intelligence platform that enables organizations to collect, process, and analyze potential security threats in their network security systems. Organizations can investigate security threats and vulnerabilities based on various parameters and identify threat patterns, behavior, and risks. If the organizations proactively detect security threats, they can improve their security plan against emerging cyber-attacks.

Administrators must observe how the organizations leverage the threat intelligence. They can analyze all sessions of the organizations and whether any organizations are inactive. This analysis can help the administrators to promote the threat intelligence to the organizations in various ways.

Intended Audience

This guide is intended for the following audience:

- Internal-Admin
- Super-Admin

System Requirements

Threat Control System is a web-based portal. The web portal can run on any latest browser including,

- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Authentication

Identity provider keys are required to authenticate the Threat Control System administrators and users. You can use either one of the following identity providers (IDP):

- Keycloak IDP
- Okta IDP
- Azure IDP

Logging using Organization's Keycloak

To log in to the Threat Control System portal using the Organization's Keycloak IDP:

1. Go to www.defend.a10networks.com.
2. Enter the organization name and click **Next**.

NOTE: The organization name is the name of the entity that purchases the threat insight intelligence application.

3. Enter your username or email address, password, and then click **Sign In**.
4. Click the product name to enter the Threat Control System application.

Logging using Single Sign On (SSO)

To log in to the Threat Control System portal using Single Sign On (SSO) with Azure IDP or Okta IDP:

1. Go to www.defend.a10networks.com.
2. Enter the organization name and click **Next**.

NOTE: The organization name is the name of the entity that purchases the threat insight intelligence application.

3. Enter your corporate email address and click **Next**.
4. Enter your corporate password and click **Sign In**.
5. Click **Yes**.

User Accounts

This chapter describes the user types and their privileges.

The following topics are covered:

User Types 9
Prerequisites 10

User Types

Threat Control System allows creating users with Role-Based Access (RBA) privileges. During the onboarding process, users are added to a specific group that grants them access privileges. The following user groups are available:

- Internal-Admin
- Super-Admin
- General-User

The following table describes the users and their privileges based on their roles:

Table 1 : Role-based Users and their Privileges

User Types	Access to Threat Control System Features	Ability to Generate and View Analytics and Reports	Access to Features in Administration Section
Internal-Admin	✓	✓	Audit Trail, Feature Flag, Notification Management, Open search Management, Session Management, Organization Onboarding, User Behavior Analytics, and User Management.
Super-Admin	✓	✓	Audit Trail, Notification

Table 1 : Role-based Users and their Privileges

User Types	Access to Threat Control System Features	Ability to Generate and View Analytics and Reports	Access to Features in Administration Section
			Management, Open Search Management, Organization Info, and User Management.
General-User	✓	✓	X

NOTE: To know how to use the Threat Control System application, see *SecDevice User Guide*.

Prerequisites

Users can be onboarded by the users who have the Internal-Admin privileges or by the support team.

To onboard a user, see the "Onboarding an Organization" section in the *SecDevice Onboarding Guide*.

Administration Tasks

In the Administration section, Internal-Admin can perform various tasks such as view and edit organization information, view Audit Trail, manage users and sessions, and onboard new organizations.

The following topics are covered:

Organization Info 12
Audit Trail 12
Searching Audit Record of a User 12
Feature Flag 13
Enabling Features 13
Notification Management 15
Adding Notifications 15
Open Search Management 17
Adding Policies 17
Viewing Indices 19
Session Management 19
Viewing Session Management 20
Cancelling a Session 20
Searching for a Session 20
Enabling Search Factors for User Sessions 21
Organization Management 21
Viewing Organizations 22
Searching for Organizations 23
Enabling Search Factors for Organizations 24
Adding Organizations 24
User Behavior Analytics 24
Viewing User Insights 25
User Management 27

Users 28
User Groups 32
IDP Groups 34
Auth Users 36
Service Account 38

Organization Info

Organization Info allows you to edit the organization information if a modification is required.

NOTE: Only the users with the admin privilege can edit the organization information.

To edit the organization information:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Organization Info**.

   Make sure that you have selected the organization that you want to edit.

3. On the **Edit Organization** screen, edit the information that you want.
4. Click **Submit**.

Audit Trail

The Audit Trail log captures the history of all actions performed by users within an organization in Threat Control System. It includes information such as actions performed by different users, their timestamp, and other relevant details.

Searching Audit Record of a User

To search for an action performed by a user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Audit Trail**.
3. Select an organization from the **Select Organization** drop-down list, available on the top-right side.
4. On the **Search Audit Logs** screen, enter either a username, a module, an action, or a URL.

   You can search your Audit Trail log by a username, an action performed, a module, or a URL such as Organization Authentication.
5. In the **Select a Date Range** drop-down list, select a date. You may enter the start and end dates of your choice, if required.
6. Click **Search Results**. This audit report appears that displays which users used certain modules and the action they performed.

   You can export the audit report of a user using the **Export CSV** option.

   To make a new search, you can click the expand arrow for the **Search Audit Logs** option to open the search panel.

Feature Flag

This chapter describes the features that are available exclusively only to specific organizations. These features can be conditional and added or removed as required.

NOTE: This feature is available to the Super-Admin only.

The following topics are covered:

Enabling Features 13

Enabling Features

Feature Flag allows you to turn certain features on and off as per your requirement. You can turn on or turn off a feature in real time, without deploying any code. This allows for better control of the features.

These features are like conditional features and help to reduce frequency of deployment and rolling back of a feature as per requirement.

To enable a feature:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Feature Flag**. The following information appears.

Table 2 : Feature Flag Details

Headings	**Description**
Feature Name	Displays the feature name.
Enabled	Displays whether a feature is enabled.
Feature Type	Displays the feature type, whether the feature belongs to a platform or a product.
Strategy Base	Displays the feature strategy.
Products	Displays the product names.
Organizations	Displays the organization name to which the feature is available.
Feature URL	Displays the URL link where a feature has been added. To go to the relevant section, click the link.
Action	Under the **Action** column, you can edit the feature name, enable or disable a feature, and delete a feature. You can change or add the products and organizations if a feature belongs to a platform. However, you can change or add the organizations only if a feature belongs to the product.

3. Click **New Feature**.
4. On the **Create New Feature** page, configure the fields as follows:

Table 3 : Feature Flag fields

Fields	**Description**
Feature Name	Enter a feature name. A feature may belong to a product such as Threat Control System or a platform within the Threat Control System application as a feature type. You

Table 3 : Feature Flag fields

Fields	Description
	can add a new feature only to a product.
Choose Product	Select a product from the **Choose Product** drop-down list. You can add multiple products.
Choose Organization	Select an organization from the **Choose Organization** drop-down list. The list displays all the onboarded organizations to the Threat Control System application.
Feature URL	Enter the route where the feature is located.
Feature Enable	Turn on **Feature Enable** to activate the new feature. **NOTE:** If required, you can disable this feature in the same way.
Save	Click **Save** to save your setting.

The feature is added to the relevant section such as service account, user authorization, notification management, or search management based on the type of the feature function.

If you want to change your search result, you can use the filter option.

Notification Management

Notification Management allows you to add notifications that are intended for organizations to inform them about new system updates, products, and organizations.

The following topics are covered:

Adding Notifications 15

Adding Notifications

You can add notifications to inform organizations about their license or product expiry, or if there is any change in the system.

To add a notification:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Notification Management**. The following information appears.

Table 4 : Notification Management

Headings	Description
Severity	Displays message severity, with high or low importance.
Status	Displays if the notification is enabled or disabled.
Message	Displays the message of the notification.
Frequency	Displays the frequency when the notification is scheduled to be sent.
Audience Scope	Displays the reason the notification is to be sent. The reason can be related to system, product, or organization types. If the system type is selected, the notification may be intended for all organizations. If the product type is selected, the notification may be intended for those organizations who have subscribed to the product. If the organization type is selected, the notification is intended for the people who belong to the selected organization.
Audience	Displays the organization or people in an organization to whom the notification is to be sent.
Created Date	Displays when the notification was created.
Modified Date	Displays if the notification was ever modified.
Action	Allows you to enable or disable the notification.

3. Click **Create Notification**.
4. On the **Create Notification** page, configure the following fields:
   a. Write a message for the notification.
   b. Select the severity such as **High** or **Low**.
   c. Set the schedule whether the notification should be sent once only, or it

should be sent on a recurring frequency.

If you schedule to send the notification One Time, you must set the real time or specific date and time. If you select Recurring frequency, you must set the specific date and time and frequency such as Daily, Monthly, and Weekly.

d. Select one of the audience scopes from System, Product, and Organization.
e. Select the audience to whom you want to send the notification.
f. Enable the notification under Status to send as per the schedule.

5. Click **Submit** to save the notification.

Open Search Management

Open Search Management allows you to add policies such as the duration for retaining the organization data in the system.

The following topics are covered:

Adding Policies 17
Viewing Indices 19

Adding Policies

You can add polices for collecting organization data from the audit log and retaining it in an index. The policy can also define the time when the index should stop gathering data. You must consider creating multiple indices to avoid overwhelming traffic to a single index.

To add a policy:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Open Search Management > Policies**. The following information appears.

Table 5 : Feature Flag Details

Headings	Description
Policy ID	Displays the Policy ID.

Table 5 : Feature Flag Details

Headings	Description
Description	Displays the description of the policy.
Applicable on	Displays organizations to which the policy is effective.
Data Retention	Displays the duration for retaining organization data in an index.
Index Rollover	Displays whether the rollover of data gathering is applicable to an index.
Created Date	Displays the date when the policy was created.
Modified Date	Displays whether the policy was ever modified.
Action	Allows you to modify the policy details or delete a policy.

3. Click **Create New Policy**.
4. On the **Create Policy** page, configure the fields as follows:
   a. Enter a **Policy ID**. You can create a policy to gather the audit log for an organization for a certain period.
   b. Add a policy description. The policy description should be identical for the specific purpose.
   c. Select one of the policy types from **Data Retention** to save data for a specific time and **Index Rollover** to stop saving the data in the specific index after a period.

      - **Data Retention**: If you select Data Retention, set indexing age as to how long the audit log should be retained in an index.
      - **Index Rollover**: If you select Index Rollover, you must also set the minimum indexing age in hours or days, minimum document count that is the audit logs count, and minimum index size in MB or GB. If a policy is assigned the rollover age, audit data gathering will automatically switch to another index after the set limits.

   d. Select an **Organization** to which the policy needs to be applied.
   e. Select the **Indices**.

      Indices are displayed from the indices list.

5. Click **Submit** to save the policy.

Viewing Indices

To view indices:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Open Search Management > Indices**. The following information appears.

Table 6 : Feature Flag Details

Headings	Description
Index Name	Displays the index name. These indices are created from audit log scheduler and added to the indices list automatically.
Status	Displays the status whether the index is active or inactive.
Created Date	Displays when the index was created.
Modified Data	Displays if the index detail was ever modified.
Last Modified By ID	Displays if the index detail was ever modified by ID.
Action	Allows to modify the policy ID.
Filter	Allows you to search for an index, by index name and status.

Session Management

The Session Management screen displays the list of current sessions and the history of the logged in sessions.

The following topics are covered:

Viewing Session Management 20
Cancelling a Session 20
Searching for a Session 20

Enabling Search Factors for User Sessions 21

Viewing Session Management

To view the sessions:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Session Management**.

   The user session screen displays the email addresses, total sessions, average session duration, last activity time, last activity URL, login time, logout time, status of the users, and session status. You can close a running session, if required.

   If you want to change your search result, you can use the filter option.

   To view further details of a session, click anywhere on the session information.

Cancelling a Session

You can cancel a running session if required.

To cancel a session:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Session Management**.
3. On the **Session Management** screen, click the **Cancel** icon available next to the user.
4. To confirm your action, click **Confirm**.

   The selected session is cancelled.

Searching for a Session

If there are hundreds of sessions and you want to view the session of a certain user, you can do so by using the filter option.

To search for a session:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Session Management**.
3. Click the **Filter** or **Filter by columns** icon on the upper-right corner on the **Users Sessions** screen.
4. Enter any of the following search filters:
   - Email
   - Group Name
   - Date Range
   - Last Activity
   - Status
5. Press **Enter**. The search result appears.

Enabling Search Factors for User Sessions

You can associate user sessions based on different factors including Email, Group Name, Login Time, Logout Time, Last Activity Time, Status, and Cancel Session. These factors help you identify a user session easily.

To enable a column:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Session Management**.
3. Click the **Hidden Column** icon available on the upper-right corner on the **Users Session** screen.
4. Select the search filters that you want to enable.

   The enabled factors are displayed in the filter criteria for sessions.

Organization Management

The **Organization Management** screen displays all the organizations onboarded to Threat Control System.

NOTE: Only the Super-Admins have the privilege to view the organization details and onboard new organizations.

The following topics are covered:

Viewing Organizations 22
Searching for Organizations 23
Enabling Search Factors for Organizations 24
Adding Organizations 24

Viewing Organizations

To view all the organizations:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Organization Management**. The following information appears.

Table 7 : Organization Details

Headings	Description
Organization Name	Displays the organization name.
Company Name	Displays the company name.
Country	Displays the country name where the company resides.
State	Displays the state name where the company resides.
Status	Displays the status whether an organization is onboarded or is inactive.
Created Date	Displays the date when an organization was onboarded.
Modified Date	Displays the date when the organization information was last modified.
Phone	Displays the phone number of the company.
Primary Contact	Displays the primary contact number of the company.
City	Displays the city name where the company resides.

Table 7 : Organization Details

Headings	Description
Street	Displays the street name where the company resides.
Industries	Displays the industries the company belongs to.
IP Addresses	Displays the IP addresses the company uses.
Action	Displays action option such as you can edit the organization information.

To view further details of an organization, click anywhere on the organization information.

Searching for Organizations

If there are hundreds of organizations and you want to view the information for an organization, use the filter option.

To search for an organization:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Organization Management**.
3. Click the **Filter** or **Filter by columns** icon on the upper-right corner on the **Organization Management** screen.
4. Enter any of the following search filters:
    - Organization Name
    - Company Name
    - Country
    - State
    - Status
5. Press **Enter**. The search result appears.

Enabling Search Factors for Organizations

You can associate organizations based on different factors including Organization Name, Company Name, and other factors. These factors help you easily identify an organization.

To enable a column:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **Organization Management**.
3. Click the **Hidden Column** icon available on the upper-right corner on the **Organization Management** screen.
4. Select the search filters that you want to enable.

   The enabled factors are displayed in the filter criteria for the organizations.

Adding Organizations

The organizations can be onboarded either by the Threat Control System support team or the organizations themselves. An organization is an entity that purchases the Threat Control System application.

NOTE: Only the users with the Internal-Admin privilege have access to this feature.

To know how to onboard an organization to the Threat Control System application, see *SecDevice Onboarding Guide*.

User Behavior Analytics

User Behavior Analytics is a technique to gather and analyze user onboarding journey and user behavior within a product. User analytics depicts whether the organizations and users are actively engaged after onboarding and how they explore different features. This analytics gives a holistic picture of product adoption and helps administrators to enhance engagement and retention of Threat Control System.

User Behavior Analytics records user behavior to identify feature usability like why the organizations and users prefer specific features over others and how long they remain engaged in the features. This smart user analytics can predict the requirements of customers and help Threat Control System to improve the features and product to meet their requirements.

Administrators can make data-driven decisions to enhance Threat Control System based on these insights.

- **Identifying Active Organizations and Users**: Knowing which organizations and users are most active helps the administrators offer additional support to high-value organizations. The administrators can also engage with less active users to understand their needs better.
- **Feature Promotion**: If certain features see high utilization, administrators can promote them further, enhancing user experience and satisfaction. Additionally, administrators can analyze why these features are preferred and use that knowledge to improve other features.
- **Feature Phasing**: If certain features are underutilized, administrators can consider phasing them out or improving their functionality based on user feedback.

NOTE: This feature is available to Internal-Admin only.

Viewing User Insights

To view the insights of users:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Behavior Analytics**. The following information appears.

Table 8 : User Analytics

User Segments	Analytic
Total Organizations	Reflects the total number of organizations that have been onboarded during a specific period.
Active Organizations	Identifies the number of organizations actively utilizing Threat Control System. Administrators can analyze which organizations are more engaged and plan to promote

Table 8 : User Analytics

User Segments	Analytic
	Threat Control System to less active organizations in effective ways.
Total users for Selected Organizations	Provides the number of users onboarded to the selected organizations.
Active users for Selected Organizations	Gives an overview of the number of users actively taking advantage of the threat intelligence by using specific features.
Feature Name	Allows the administrators to discern the features of Threat Control System that are being used more often by users of the selected organizations with their engagement counts. This analysis helps the administrators tailor the Threat Control System application to the needs of the organizations.
Engagement Count	Gives an insight about which features are being used more often.

3. Select an organization from the **Select Organization** drop-down list, available on the top-right side.

   You can select multiple organizations. **All Organizations** is selected by default.

4. Select a duration from the **Select Duration** drop-down list.

   Following are the available periods 7 Days, 15 Days, 30 Days, 45 Days, 60 Days, 90 Days, and Custom.

   The **7 Days** option is selected by default. If you select the **Custom** option, you can select a maximum of 90 days as a date range for your report.

   Usage of different features of an organization appears. This usage shows engagement counts for each feature. If you want to investigate the insights for a specific feature or a user, you can search using the filter option.

The Active Organizations, Total users for Selected Organizations, Active users for Selected Organizations, and Usage details of Defend options reflect the insights based on the selected organizations and period.

User Management

User Management allows you to add a new user, a new group, a new IDP group, a new auth user, a new service account, and edit the information related to them. To view User Management:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**. Following are the options under user management.
   - User Groups — Displays all the listed user groups.
   - Users — Displays all the listed users.
   - IDP Groups — Displays all the listed IDP groups.
   - Auth Users — Displays all the listed auth users.
   - Service Account — Displays all the listed service accounts.

The following topics are covered:

Users 28
Adding Users 28
Editing a User 29
Blocking or Unblocking a User 30
Inactivating a User 30
Searching for a User 31
Enabling Search Factors for Users 31
User Groups 32
Adding User Groups 32
Searching for a User Group 33
Enabling Search Factors for User Groups 34
IDP Groups 34
Adding IDP Groups 35

Searching for an IDP Group 35
Enabling Search Factors for IDP Groups 36
Auth Users 36
Adding Auth Users 37
Service Account 38
Adding Service Accounts 38
Creating Access Token for APIs 39

Users

The Users tab allows you to add new users, edit user information, and manage users in the Threat Control System application.

The following topics are covered:

Adding Users 28
Editing a User 29
Blocking or Unblocking a User 30
Inactivating a User 30
Searching for a User 31
Enabling Search Factors for Users 31

Adding Users

To add a new user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the User Management screen, click the **Users** tab. The following information appears.

Table 9 : User Details

Headings	Description
First Name	Displays the first names of the users.

Table 9 : User Details

Headings	Description
Last Name	Displays the last names of the users.
Email	Displays the email addresses of the users.
Groups	Displays the groups to which the users belong. The user groups are Internal-Admin, Super-Admin, General-User.
Created Date	Displays the date when a user was added in Threat Control System.
Modified Date	Displays the date when any user information was modified.
Auto Created	Indicates whether the user was automatically added to the Threat Control System application, or the user was added by the A10 Support team.
Status	Displays whether a user is active or inactive.
Action	Allows you to edit the user details, block a user, or inactivate a user.

4. Click the **New User** button.
5. On the **Create New User** screen, enter **First Name**, **Last Name**, **Email**, and then select a **Group**. You can select multiple groups if required. Following are the groups available by default:
   - Internal-Admin
   - Super-Admin
   - General-User

NOTE: To know more about the user types, see User Types.

6. Click **Save**.

Editing a User

To edit a user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **Users** tab.
4. Under the **Action** column, click the **Edit** icon available to a user.
5. On the **Edit User** screen, edit the first name, last name, email address, and group as required.
6. Click **Update**.

Blocking or Unblocking a User

Administrators can block users temporarily. However, the blocked users can be unblocked if required.

To block a user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **Users** tab.
4. Under the **Action** column, click the **Block** icon available to a user.
5. To confirm your action, click **Yes**.

   The selected user is blocked. An **Unblock** icon appears to the user. An option to send an email notification about the user being blocked also appears.

6. To send an email notification, click **Submit Email**. If you do not want to send the email notification, click **Do Not Submit Email**.

NOTE: If you require to unblock a user, click the **Unblock** icon.

Inactivating a User

Administrators can deactivate users who have left their organization to prevent their access to the Threat Control System application.

To inactivate a user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **Users** tab.
4. Under the **Action** column, click the **Inactivate** icon available to a user.
5. To confirm your action, click **Delete**.

   The selected user is deactivated immediately.

Searching for a User

To find detailed information about a user, use the filter option.

To search a user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the User Management screen, click the **Users** tab.
4. Click the **Filter** or **Filter by column** icon available on the upper-right corner on the **User Management** screen.
5. Enter any of the following search filters:
   - First Name
   - Last Name
   - Email
   - Groups
   - Auto Created
   - Active
6. Press **Enter**. The search result appears.

   To view further details of a user, click anywhere on the user information.

Enabling Search Factors for Users

You can associate users based on different search factors, including First Name, Last Name, Email, Groups, Created Date, Modified Date, Auto Created, and Action. These factors help you identify a user easily. To associate users by these factors, you can enable them in the Hidden Column.

To enable a column:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **Users** tab.
4. Click the **Hidden column** icon available on the upper-right corner on the **User Management** screen.
5. Select the search filters that you want to enable.

   The enabled factors are displayed in the filter criteria for the users.

User Groups

The User Groups tab allows you to add new groups, edit group information, and manage groups in the Threat Control System application.

The following topics are covered:

Adding User Groups 32
Searching for a User Group 33
Enabling Search Factors for User Groups 34

Adding User Groups

To add a new user group:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the User Management screen, click the **User Groups** tab. The following information appears.

Table 10 : User Groups

Headings	Description
User Group Name	Displays the groups added in the Threat Control System application.
IDP User Groups	Displays the IDP user groups.
Created Date	Displays the date when a group was created.
Modified Date	Displays the date when a group information was modified.
Action	Allows you to edit and delete the user group information.

4. Click the **New Group** button.
5. On the **Create New Group** screen, enter a Group Name and then select an IDP Group. Following are the available groups by default:
   - Internal-Admin
   - Super-Admin
   - General-User

NOTE: To know more about the user types, see User Types.

6. Click **Save**.

Searching for a User Group

To find detailed information about a user group, use the filter option.

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **User Groups** tab.
4. Click the **Filter** or **Filter by column** icon available on the upper-right corner on the **User Management** screen.
5. Enter any of the following search filters:

- User Group Name
- IDP User Groups

6. Press **Enter**. The search result appears.

   To view further details of a user group, click anywhere on the user group information.

Enabling Search Factors for User Groups

You can associate user groups based on different search factors, including User Group Name, IDP User Groups, Created Date, Modified Date, and Action. These factors help identify a user group easily. To associate user groups by these factors, you can enable them in the Hidden Column.

To enable a column:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **User Groups** tab.
4. Click the **Hidden column** icon available on the upper-right corner on the User Management screen.
5. Select the search filters that you want to enable.

   The enabled factors will be displayed in the filter criteria for the user groups.

IDP Groups

The IDP Groups tab allows you to add new IDP groups, edit IDP group information, and manage IDP groups in the Threat Control System application.

The following topics are covered:

Adding IDP Groups 35
Searching for an IDP Group 35
Enabling Search Factors for IDP Groups 36

Adding IDP Groups

To add a new IDP Group:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the User Management screen, click the **IDP Groups** tab. The following information appears.

Table 11 : IDP Groups

Headings	Description
IDP Name	Displays the IDP names that can be any one of the following: Keycloak, Okta, and Azure.
IDP User Group Identifier	Displays the IDP user group identifier of the respective IDPs.
IDP User Group Name	Displays the IDP user group name.
User Group Name	Displays the user group name.
Action	Allows you to edit and delete the IDP group information.

4. Click the **New IDP Group** button.
5. On the **Create New IDP Group** screen, select an **IDP name**.
6. Enter **IDP Group Identifier** and **IDP Group Name**.
7. Select a **User Group**.
8. Click **Save**.

Searching for an IDP Group

To find detailed information about an IDP group, use the filter option.

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **IDP Groups** tab.

4. Click the **Filter** or **Filter by column** icon available on the upper-right corner on the **User Management** screen.
5. Enter any of the following search filters:
    - IDP Name
    - IDP User Group Identifier
    - IDP User Group Name
    - User Group Name
6. Press **Enter**. The search result appears.

    To view further details of an IDP Group, click anywhere on the IDP Group information.

Enabling Search Factors for IDP Groups

You can associate IDP groups based on different search factors, including IDP Name, IDP User Group Identifier, IDP User Group Name, User Group Name, and Action. These factors help identify an IDP group easily. To associate the IDP groups by these factors, you can enable them in the Hidden Column.

To enable a column:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **IDP Groups** tab.
4. Click the **Hidden column** icon available on the upper-right corner on the User Management screen.
5. Select the search filters that you want to enable.

    The enabled factors will be displayed in the filter criteria for the IDP groups.

Auth Users

An Auth User is a user who can configure the security devices with the Threat Control System APIs to automatically download the IP Block Lists on the security devices. After you create an auth user, you can go to the security devices that you use in your network environment and configure the security device with the auth user credentials. To know how to configure a security device, see Configuring Security Devices.

The Auth Users tab allows you to add new authentication users, edit authentication users' information, and manage the authentication users in the Threat Control System application.

NOTE: This feature is available based on the license subscription of an organization.

The following topics are covered:

Adding Auth Users 37

Adding Auth Users

To add a new auth user:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **Auth Users** tab. The following information appears.

Table 12 : Auth User Details

Headings	Description
First Name	Displays the first name of an auth user.
Last Name	Displays the last name of an auth user.
Email	Displays the email address of an auth user.
Username	Displays the username of an auth user.
Groups	Displays the group name of an auth user.
Created Date	Displays the date when an auth user was added in Threat Control System.
Action	Allows you to edit the auth user details and delete an auth user.

To view further details of an auth user, click anywhere on the auth user information.

4. Click the **New Auth User** button.
5. On the **Create New User** screen, enter **First Name**, **Last Name**, **Username**, and **Email** address.
6. Select a **Group** name and then enter a **Password**.
7. Click **Save**.

   An Auth User account is created. Save the credentials. Using the Auth User credentials, you can configure the security device. To know how to configure a security device, see Configuring Security Devices.

Service Account

A service account allows you to create an authenticated user account to connect with the APIs. This service account allows to connect with any kind of APIs.

The Service Account tab allows you to add new service account, edit the service account information, and manage the service account.

NOTE: This feature is available based on the license subscription of an organization.

The following topics are covered:

Adding Service Accounts 38
Creating Access Token for APIs 39

Adding Service Accounts

To add a new service account:

1. On the **Home** page, click the **Hamburger** menu.
2. Click **User Management**.
3. On the **User Management** screen, click the **Service Account** tab. The following

information appears.

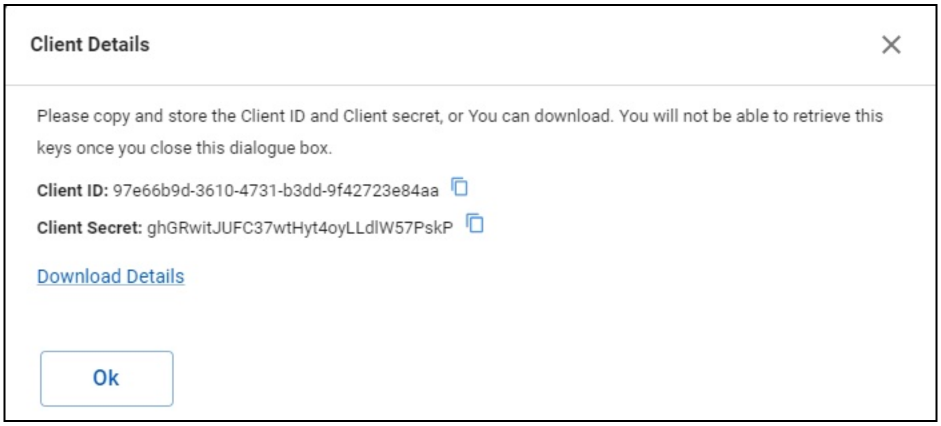
Table 13 : Service Account Details

Headings	Description
Name	Displays the full name of a service account user.
Description	Displays the description of the service account.
Client ID	Displays the Client ID of the service account user.
Action	Allows you to delete a service account.

To view further details of a service account, click anywhere on the service account information.

4. Click the **+Create Service Account** button.
5. On the **Create Service Account** screen, enter **Name** of the service account user and **Description** of the service account.
6. Click **Save**.

Figure 1 : Client Details



Client Details

Please copy and store the Client ID and Client secret, or You can download. You will not be able to retrieve this keys once you close this dialogue box.

Client ID: 97e66b9d-3610-4731-b3dd-9f42723e84aa

Client Secret: ghGRwitJUFC37wtHyt4oyLLdlW57PskP

Client ID and Client Secret are created. Use these credentials to create an access token with Keycloak to access the Threat Control System APIs.

Creating Access Token for APIs

To create an access token:

1. Go to https://keycloak.a10networks.com/realms/<organizationName>/protocol/openid-connect/token.

   Replace <*organizationName*> with the actual organization name.

2. Under **Body**, pass **--data-urlencode 'grant_type=client_credentials'**.

   Replace client credentials with the basic authorization credentials that were generated while creating a service account, as described in the Adding Service Accounts section.

   An access token is created. Use this access token to access the Threat Control System APIs. Our organization provides the APIs.

   For more information about how to onboard a new organization, see *SecDevice Onboarding Guide*.

Support to Add IP Blocklists to Network Devices

Threat Control System enables you to seamlessly download the IP Block Lists on your security devices to block potentially malicious IP addresses. It enables secure and efficient downloading of IP Block Lists over HTTPS.

You can configure the IP Block List URL with the credentials of an auth user on your security devices and enable them to automatically retrieve and update the IP Block Lists at regular intervals. Threat Control System supports both A10 and non-A10 security devices.

This section includes the following topics:

How It Works

A non-A10 firewall or other security device should be able to:

- Download specific IP Block Lists such as threat lists, network vs. host lists, and specific size-variants of these lists from an externally exposed API endpoint available to the customers.
- Download the IP Block Lists over HTTPS.
- Support the IP Block Lists in a text file and STIX file.
- Support automatic download of the IP Block Lists periodically.

Entitlement & Security

- Threat Control System authenticates every download request to verify customer entitlement. For example, the customers must have an active subscription with Threat Control System. If the subscription of a customer has expired, a message “You do not seem to have a license for this feature.” is displayed.
- HTTPS basic authentication using the username and password is supported.
- The user’s API request to download the IP Block Lists will be authenticated against the same user credentials that they use to access the Threat Control System application.
- Use standard HTTPS responses to return an error if the credentials provided by Threat Control System do not match.

The following topics are covered:

Prerequisites 42
Types of IP Block Lists and Their Usage 42
Configuring Security Devices 49
Viewing the Blocked IP Addresses 52
Creating Security Policies 54
API List 54

Prerequisites

To configure non-A10 security devices, the following prerequisites must be met:

- User Credentials: User credentials of the auth user account. Only the security devices that support HTTPS basic authentication using username and password are supported. To know more about how to create an auth user account, see Auth Users.
- API: API to configure external connectors. Our organization will provide the APIs to the organizations. To see the list of APIs, see API List.

Types of IP Block Lists and Their Usage

Following are the types of IP Block Lists that Threat Control System can block.

A10-Block-Bot-Activity

The A10-Block-Bot-Activity list consists of IP addresses that are known to be part of DDoS botnet attacks, used for launching distributed denial-of-service (DDoS) attacks. This block list tracks bots from the Mozi, Mirai, Gafgyt, RCE, and other botnet families.

Advantages of Blocking the A10-Block-Bot-Activity Lists

Following are the advantages of blocking the A10-Block-Bot-Activity lists.

- Identify the source of potential DDoS attack traffic.
- Block traffic from DDoS botnets.

- Protect the networks from malicious/unnecessary traffic.

Application of the A10-Block-Bot-Activity Lists

Organizations may choose to apply the A10-Block-Bot-Activity lists in any of the following ways:

- Configure the A10-Block-Bot-Activity lists on routers, firewalls, and edge devices to block malicious traffic.
- Configure the A10-Block-Bot-Activity lists on monitoring devices to analyse traffic.
- Use the A10-Block-Bot-Activity lists in forensic investigations to identify infected systems.

Types of the A10-Block-Bot-Activity Variants

The A10-Block-Bot-Activity list can be in any of the following variants.

- Full (can contain over 1m IP/Subnets)
- Curated to 100k IP/Subnets
- Curated to 10k IP/Subnets

The A10-Block-Bot-Activity lists are available in three sizes for the purposes of loading lists on devices with limited capacity. Although it is optimal to use the full list, the smaller lists are filtered to contain botnet IPs that are considered more critical due to recent activity.

Use Cases

Following may be use case scenarios.

- Network administrators can configure their edge firewall to block all traffic from the IP addresses in the A10-Block-Bot-Activity lists. This helps to protect the organizations' network from DDoS attack traffic generated by compromised computers and Internet-of-Things (IoT) devices.
- A university administrator uses the A10-Block-Bot-Activity list to evaluate if any of the IP addresses in the list belong to the university’s network. This helps to identify compromised systems and initiate remediation actions.

Traffic Flow for the A10-Block-Bot-Activity Lists

Organizations can use a firewall or intrusion detection system (IDS) to apply the A10-Block-Bot-Activity list.

Table 14 : Traffic Flow

Inbound vs Outbound	Block vs Monitor (Detect)	How to Apply
Inbound	Block / Monitor	Add the A10-Block-Bot-Activity list to the firewall's blacklists.
Inbound	Block / Monitor	Use a security appliance that automatically blocks traffic from the blocklists.
Outbound	Monitor	Monitor firewall logs (on a SIEM) for connections from internal machines to any of these botnet IP addresses on the Internet to determine if internal systems are compromised.

A10-Block-C2-Servers

The A10-Block-C2-Servers list consists of IP addresses that are known to be used as Command & Control (C2) servers and malware staging servers used by botnets. C2 servers communicate with infected devices and send them instructions.

Organizations can use the A10-Block-C2-Servers list to prevent their systems from communicating with IP addresses that are known to be used by C2 servers.

Advantages of Blocking the A10-Block-C2-Servers Lists

Following are the advantages of blocking the A10-Block-C2-Servers lists.

- Identify the source of Command & Control (C2) traffic.
- Block Command & Control (C2) traffic.
- Prevent infected machines from receiving instructions from C2 servers and being used to infect other machines on the network.
- Prevent infected machines from launching DDoS attacks.
- Identify internal machines that attempt connections to C2 servers, an indicator of infection requiring remediation.

Application of the A10-Block-C2-Servers Lists

Organizations may choose to apply the A10-Block-C2-Servers lists in any of the following ways:

- Add the A10-Block-C2-Servers list to the firewall's blacklists.
- Use a security appliance that automatically blocks traffic from the blocklists.
- Write a script to check their systems for connections to IP addresses on the blocklists.

Use Cases

Following may be use case scenarios.

- Network security managers can configure their edge firewall to block all traffic to and from IP addresses in the A10-Block-C2-Servers list. This stops any infected machines on the network from communicating with C2 servers and helps prevent the machines being used for DDoS attacks.
- A government security researcher can use the A10-Block-C2-Servers list to identify and investigate potential sources of malicious C2 traffic. This information can be used to track down and disrupt DDoS botnets.

Traffic Flow for the A10-Block-C2-Servers Lists

Organizations can use a firewall or intrusion detection system (IDS) to apply the A10-Block-C2-Servers list.

Table 15 : Traffic Flow

Inbound vs Outbound	Block vs Monitor (Detect)	How to Apply
Inbound	Block / Monitor	Add the A10-Block-C2-Servers list to the firewall's blacklists.
Inbound	Block / Monitor	Use a security appliance that automatically blocks traffic from the blocklists.
Outbound	Monitor	Monitor firewall logs (on a SIEM) for connections from internal machines to any of these C2 IP addresses on the outside. That

Table 15 : Traffic Flow

Inbound vs Outbound	Block vs Monitor (Detect)	How to Apply
		would be an indicator of compromise.

A10-Block-Reflectors-Critical

The A10-Block-Reflectors-Critical lists consist of IP addresses that are known to be used as reflectors for DDoS attacks.

Reflectors are typically uninfected systems that are used by attackers to amplify the traffic of DDoS attacks, by forcing the reflectors to send unnecessary traffic to the victim’s IP address.

Advantages of Blocking the A10-Block-Reflectors-Critical Lists

Following are the advantages of blocking the A10-Block-Reflectors-Critical list.

- Identify the source of potential DDoS reflection traffic.
- Block traffic from DDoS reflectors.
- Protect their networks from the sources of DDoS reflection traffic.
- Identify reflectors within network ranges they control.

Application of the A10-Block-Reflectors-Critical Lists

Organizations may choose to apply the A10-Block-Reflectors-Critical Lists in any of the following ways:

- Add the A10-Block-Reflectors-Critical lists to their firewall's blacklists.
- Use a security appliance that automatically blocks traffic from the blocklists.
- Write a script to check their systems for connections to IP addresses on the blocklists.

Use Cases

Following may be use case scenarios.

- An organization can configure its firewall to block all traffic from IP addresses in the A10-Block-Reflectors-Critical list. This helps to protect the organization's network from DDoS attacks that use reflectors.

- A security researcher uses the A10-Block-Reflectors-Critical list to identify and investigate potential sources of DDoS attacks that may be using reflectors. This information can be used to track down vulnerable systems on the network and prevent one’s own network to be part of a reflection attack.

A10-Killnet-Block-List

The A10-Killnet-Block-List consists of IP addresses that are associated with the Killnet cyberattack group. Killnet is a pro-Russian hacktivist group that has been responsible for several cyberattacks against targets in Ukraine and other countries. This list is independent of other A10 block lists and will contain proxy IPs used by Killnet and compromised devices that form the core of the botnet.

Organizations can use the A10-Killnet-Block-List to prevent their systems from communicating with IP addresses that are a part of the Killnet botnet.

Advantages of Blocking the A10-Killnet-Block-List

Following are the advantages of blocking the A10-Killnet-Block-List.

- Identify the source of potential DDoS attack traffic from the Killnet botnet.
- Block traffic from the Killnet botnet.
- Protect their networks from malicious/unnecessary traffic.

Application of the Killnet-Block-List

Organizations may choose to apply the Killnet-Block-List in any of the following ways:

- Add the Killnet-Block-List to the firewall's blacklists.
- Use a security appliance that automatically blocks traffic from the blocklists.
- Write a script to check their systems for connections to IP addresses on the blocklists.

Use Cases

Following may be use case scenarios.

- An organization can configure its firewall to block all traffic from IP addresses in the Killnet-Block-List. This helps to protect the organization's network from malicious traffic from Killnet.

- A security researcher uses a Killnet-Block-List to identify and investigate potential sources of malicious traffic that may be associated with the Killnet group. This information can be used to track down and disrupt malicious activity.

scan-fullbogons

The scan-fullbogons list consists of all IP addresses that should not be part of the Internet’s routing tables, often referred to as “bogons”. A bogon is an IP address that is not assigned to any network or device. Attackers often use bogons to hide their malicious traffic.

Organizations can use the scan-fullbogons list to prevent their systems from accepting traffic pretending to be from a bogon network range.

Advantages of Blocking the scan-fullbogons List

Following are the advantages of blocking the scan-fullbogons list.

- Identify DDoS attack traffic pretending to be from a bogon network range.

Application of the scan-fullbogons List

Organizations may choose to apply the scan-fullbogons list in any of the following ways:

- Add the scan-fullbogons list to the firewall's blacklists.
- Use a security appliance that automatically blocks traffic from the blocklists.
- Write a script to check their systems for connections to IP addresses on the blocklists.

Use Cases

Following may be use case scenarios.

- An organization can configure its firewall to block all traffic from bogon IP addresses. This helps to protect the organization's network from accepting DDoS traffic spoofing a bogon IP.

scan-TOR

The scan-TOR list consists of IP addresses that are known to be Tor exit nodes. Tor exit nodes are the final nodes in The Onion Router (TOR) network where traffic passes through before reaching its destination. Attackers can use TOR to hide their actual network locations during reconnaissance and DDoS attacks.

Organizations can use the scan-TOR list to prevent their systems from communicating with Tor network exit nodes.

Advantages of Blocking the scan-TOR List

Following are the advantages of blocking the scan-TOR list.

- Identify traffic from the Tor network.
- Block traffic from the Tor network.
- Protect their networks from attackers communicating with their networks via Tor.

Application of the scan-TOR List

Organizations may choose to apply the scan-TOR list in any of the following ways:

- Add the scan-TOR list to the firewall's blacklists.
- Use a security appliance that automatically blocks traffic from the blocklists.
- Write a script to check their systems for connections to IP addresses on the blocklists.

Use Cases

Following may be use case scenarios.

- An organization can use the scan-TOR list to block all traffic from the Tor exit nodes. This helps to protect the organization’s networks from malicious traffic that may be originating from the Tor exit nodes. For example, a cybercriminal could use a Tor exit node to launch a denial-of-service (DDoS) attack against the company's website.
- A security researcher can use the scan-TOR list to identify and investigate potential sources of malicious traffic that may be using the Tor exit nodes. This information can be used to track down and disrupt malicious activity.

Configuring Security Devices

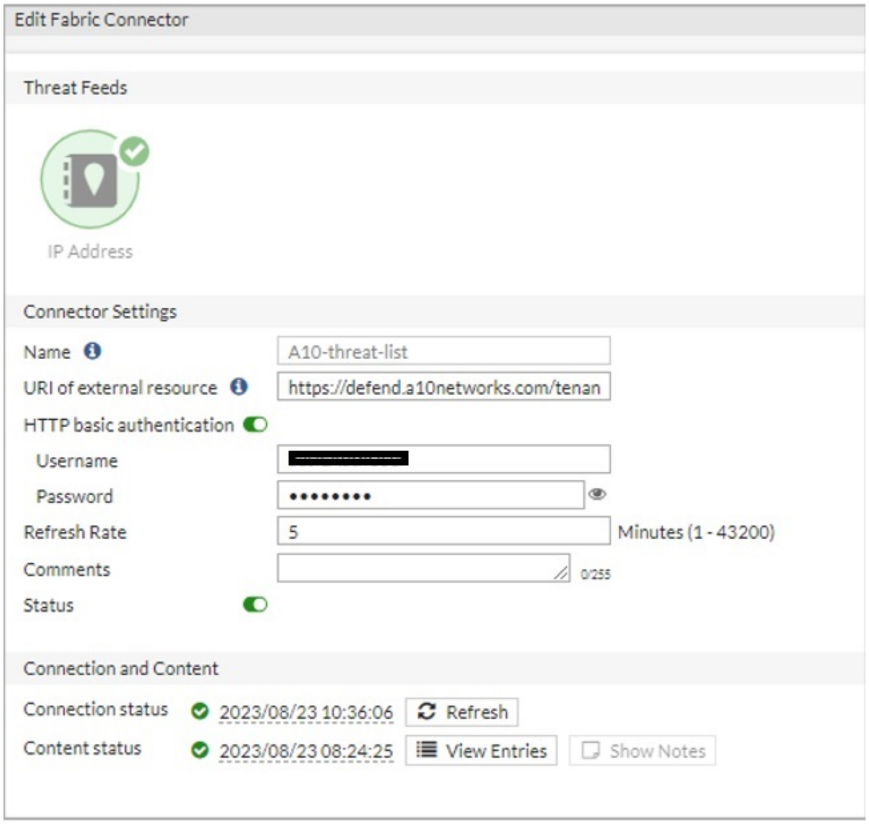
To configure the non-A10 security devices:

1. Go to your security device.

   In your security device, browse to the feature used for API configuration. Different security devices may have different names for this purpose. For example, in Fortinet devices, you may have the **Fabric Connectors** feature while in PAN devices, you may have **External Dynamic Lists**. In this example, we are displaying how to configure a Fortinet device.

   However, the following IP Block List URL interface is common in most of the security devices.

   Figure 2 : Connector Interface



Edit Fabric Connector

Threat Feeds

Connector Settings

Name: A10-threat-list
URI of external resource: https://defend.a10networks.com/tenan
HTTP basic authentication: on
Username: [redacted]
Password: ••••••••
Refresh Rate: 5 Minutes (1 - 43200)
Comments: 0/255
Status: on

Connection and Content

Connection status: 2023/08/23 10:36:06
Content status: 2023/08/23 08:24:25

2. Configure the fields as follows:

   Table 16 : Connector Fields

Fields	Description
Name	Enter a name for your setting.

Table 16 : Connector Fields

Fields	**Description**
URI of external resource	Enter an API. Use a specific API to track a specific attack. For example, use the following API to track the attacks on the command and control (C2) servers: *https://defend.a10networks.com/organization/a10networks/api/v1/threat-lists/generate/direct-download/A10-Block-C2-Servers/?country=all&format=ipv4host* To track other types of attacks, add relevant APIs to the device. You may require adding multiple APIs to track different types of attacks according to the goal of your organization. Replace the 'organization' name with the actual organization name. Threat Control System will provide the APIs to the organizations to carry out different purposes. To see the list of APIs, see API List.
Username	Enter your username. You must use the auth username and credentials to configure the security device. To know more about how to create an auth user, see Auth Users.
Password	Enter your password.
Refresh Rate	Enter time to retrieve the IP Block Lists at the assigned interval. Time is in minutes between 1 through 43200.
Comments	Enter a comment if you want. This is an optional field.
Status	Toggle the status to active.
Connection Status	Enable connection status.
Refresh	Click the **Refresh** button to update the IP Block Lists.
Content Status	Enable content status.

Table 16 : Connector Fields

Fields	Description
View Entries	Click the **View Entries** button to view the IP addresses downloaded on the security device.

The security device will synchronize with the Threat Control System application through the configured API to fetch the IP Block Lists at the configured time intervals.

For more information about IP Block List, see *SecDevice Administrator's Guide* and *SecDevice User Guide*.

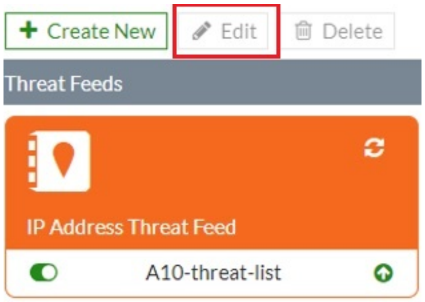
Viewing the Blocked IP Addresses

To view the blocked IP addresses:

1. Go to **Security Fabric > Fabric Connectors**.

   In this example, the Fortinet device interface is being displayed. The interface of any other security device may differ.

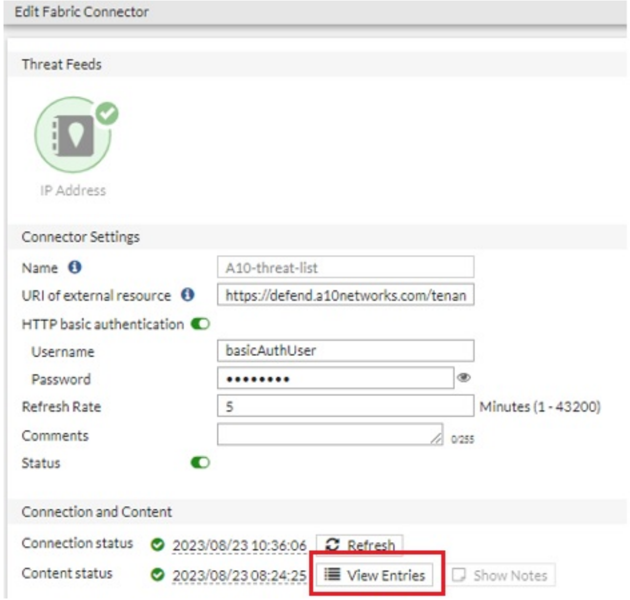
   Figure 3 : Edit Menu

2. Select a feed and click **Edit**.

   The **Last Update** field shows the date and time when the feed was last updated.

Figure 4 : View Entries



Edit Fabric Connector

Threat Feeds

Connector Settings

Name	A10-threat-list
URI of external resource	https://defend.a10networks.com/tenan
HTTP basic authentication	●
Username	basicAuthUser
Password	••••••••
Refresh Rate	5 Minutes (1 - 43200)
Comments	0/255
Status	●

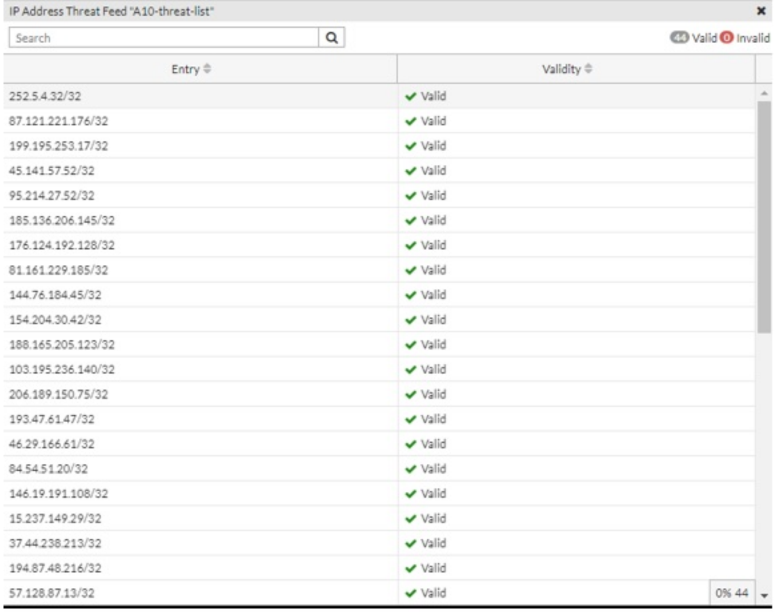
Connection and Content

Connection status	✓ 2023/08/23 10:36:06 Refresh
Content status	✓ 2023/08/23 08:24:25 View Entries Show Notes

3. Under **Content status**, click the **View Entries** button.

The blocked IP addresses are listed.

Figure 5 : Downloaded IP Lists



IP Address Threat Feed "A10-threat-list"

Entry	Validity
252.5.4.32/32	✓ Valid
87.121.221.176/32	✓ Valid
199.195.253.17/32	✓ Valid
45.141.57.52/32	✓ Valid
95.214.27.52/32	✓ Valid
185.136.206.145/32	✓ Valid
176.124.192.128/32	✓ Valid
81.161.229.185/32	✓ Valid
144.76.184.45/32	✓ Valid
154.204.30.42/32	✓ Valid
188.165.205.123/32	✓ Valid
103.195.236.140/32	✓ Valid
206.189.150.75/32	✓ Valid
193.47.61.47/32	✓ Valid
46.29.166.61/32	✓ Valid
84.54.51.20/32	✓ Valid
146.19.191.108/32	✓ Valid
15.237.149.29/32	✓ Valid
37.44.238.213/32	✓ Valid
194.87.48.216/32	✓ Valid
57.128.87.13/32	✓ Valid

Creating Security Policies

You can create security policies and apply to the IP Block Lists. To know what type of security policies you can create, check your security devices.

API List

Following is the API list that the organizations can use to configure security devices. You must use different APIs for different purposes. Change the actual organization name in place of <*organizationName*>.

Table 17 : APIs

APIs	Purpose of APIs
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/scan-fullbogons/?country=all&format=ipv4host	This API tracks the attacks of full bogon types.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/scan-TOR/?country=all&format=ipv4host	This API tracks the attacks on TOR Exit Nodes on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/scan-TOR/?country=all&format=ipv4network	This API tracks the attacks on TOR Exit Nodes in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Killnet-Block-List/?country=all&format=ipv4host	This API tracks the Killnet attack types on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Killnet-Block-List/?country=all&format=ipv4network	This API tracks the Killnet attack types in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-	This API tracks the attacks on the command

Table 17 : APIs

APIs	Purpose of APIs
lists/generate/direct-download/A10-Block-C2-Servers/?country=all&format=ipv4host	& control (C2) servers on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-C2-Servers/?country=all&format=ipv4network	This API tracks the attacks on the command & control (C2) servers in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical-10K/?country=all&format=ipv4host	This API tracks the Reflectors-Critical attacks on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical-10K/?country=all&format=ipv4network	This API tracks the Reflectors-Critical attacks in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical-100K/?country=all&format=ipv4host	This API tracks the Reflectors-Critical on a large scale on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical-100K/?country=all&format=ipv4network	This API tracks the Reflectors-Critical on a large scale in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical/?country=all&format=ipv4host	This API tracks the Reflectors-Critical on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical/?country=all&format=ipv4network	This API tracks the Reflectors-Critical in the network.

Table 17 : APIs

APIs	Purpose of APIs
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Bot-Activity-10K/?country=all&format=ipv4host	This API tracks the botnet attacks on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Bot-Activity-10K/?country=all&format=ipv4network	This API tracks the botnet attacks in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Bot-Activity-100K/?country=all&format=ipv4host	This API tracks the botnet attacks on a large scale on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Bot-Activity-100K/?country=all&format=ipv4network	This API tracks the botnet attacks on a large scale in the network.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Bot-Activity/?country=all&format=ipv4host	This API tracks the bot attacks on the IP Addresses.
https://defend.a10networks.com/organization/<*organizationName*>/api/v1/threat-lists/generate/direct-download/A10-Block-Bot-Activity/?country=all&format=ipv4network	This API tracks the bot attacks in the network.

Appendix

Managing Users in Organization's Keycloak

This section is intended for the Threat Control System administrators of your organization. The administrator can manage users and groups using organization's Keycloak.

The following topics are covered:

Logging in to Keycloak 57

Adding a New User 58

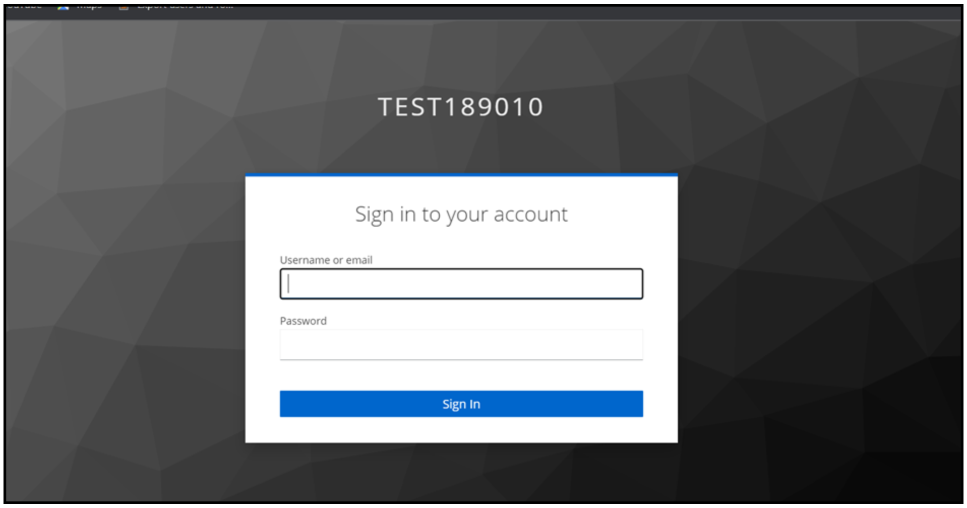
Deleting the Existing Users 62

Logging in to Keycloak

To log in to Keycloak:

1. Go to **keycloak.a10networks.com/admin/<organization-name>/console**.
2. Enter your credentials that you have received over email from the Threat Control System Support team.
3. Click **Sign In**.

Figure 6 : Logging in to Keycloak



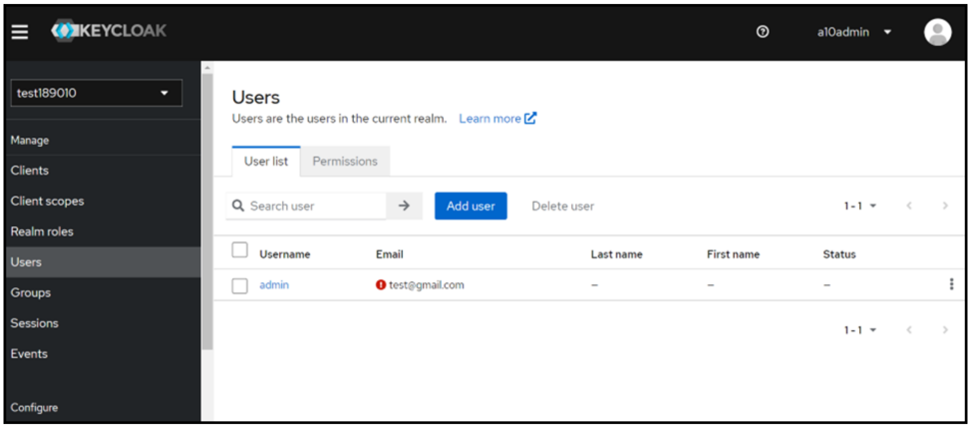
Adding a New User

To add a new user:

1. In the Keycloak console, click **Users**.

   The following screen appears.

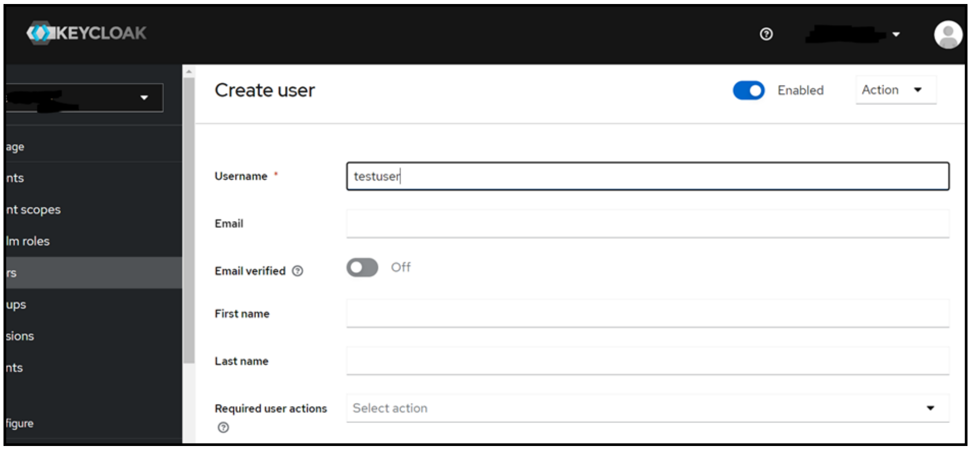
   Figure 7 : User List

	Username	Email	Last name	First name	Status
□	admin	test@gmail.com	–	–	–

2. Click **Add user**.

Figure 8 : Add User



Create user

Username * testuser

Email

Email verified Off

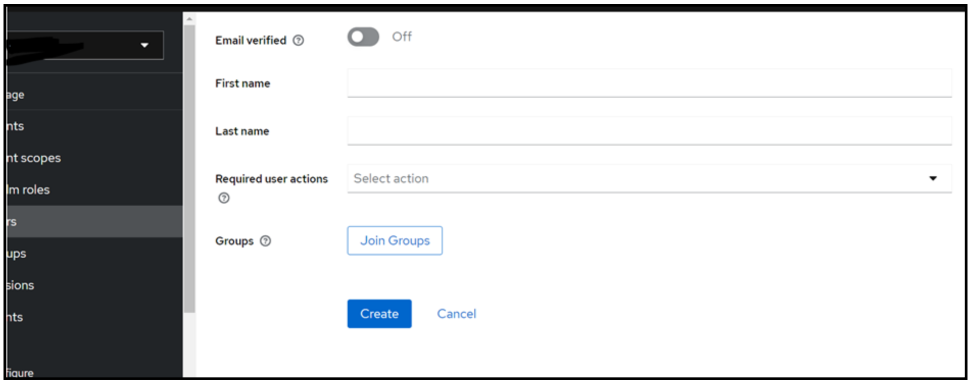
First name

Last name

Required user actions Select action

3. Enter the username and email address of the user.
4. Set **Email verified** to ON, if the entered email address is already verified.
5. Enter the first name and last name of the user.

Figure 9 : User action



Email verified Off

First name

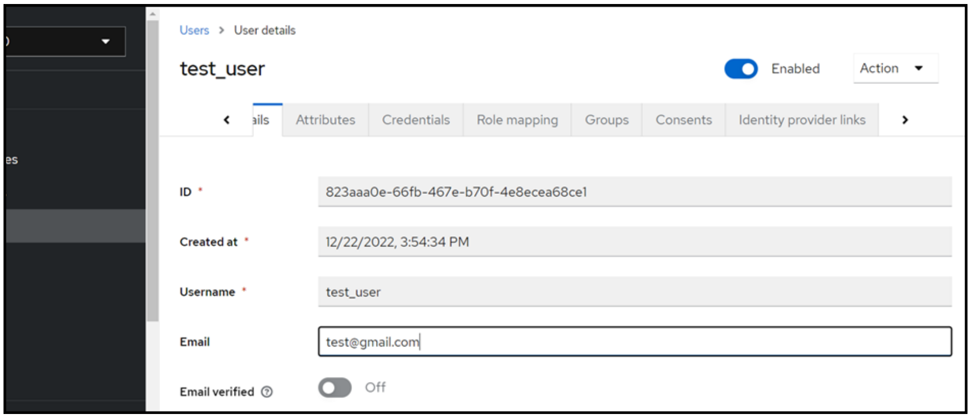
Last name

Required user actions Select action

Groups

6. Select the **Required user action** and click **Join Groups**.
7. Click **Create**.

Figure 10 : User Created



ID * 823aaa0e-66fb-467e-b70f-4e8ecea68ce1

Created at * 12/22/2022, 3:54:34 PM

Username * test_user

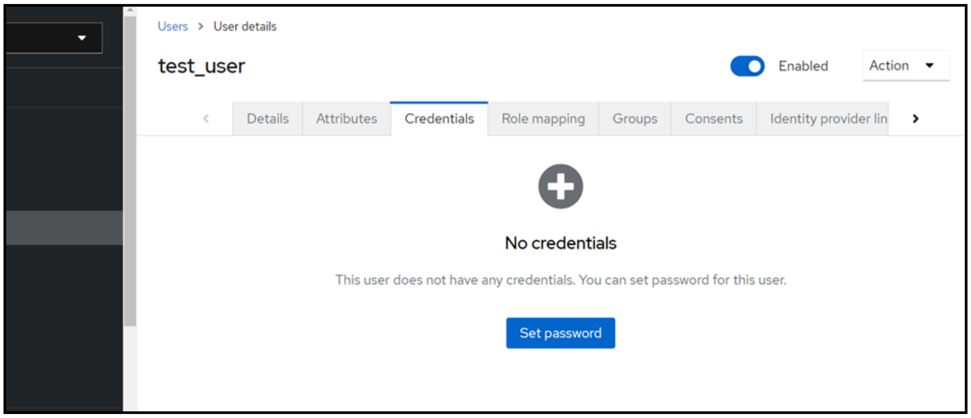
Email test@gmail.com

Email verified Off

The user is added, and a unique ID is created for the user.

8. To set the password for the user, click **Credentials**.

Figure 11 : Credentials

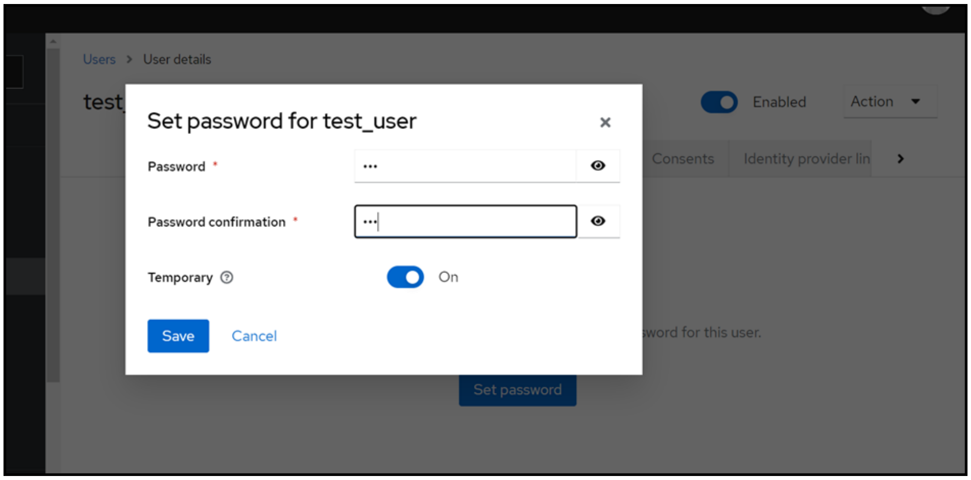


No credentials

This user does not have any credentials. You can set password for this user.

9. Click **Set password**.

Figure 12 : Set password



Set password for test_user

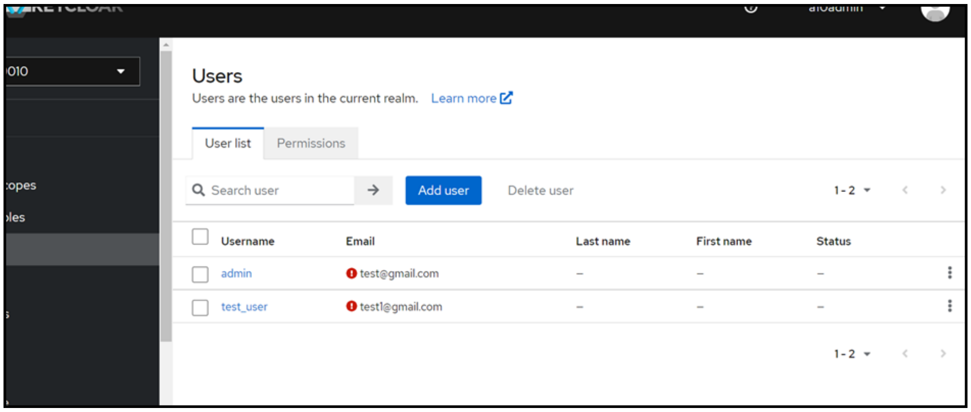
Password * ···

Password confirmation * ···

Temporary On

10. Enter a desired password.
11. To set the password temporarily, turn on **Temporary**. User will be allowed to change the password on first log in.
12. Click **Save**.

Figure 13 : User Created



Users

Users are the users in the current realm. Learn more

Username	Email	Last name	First name	Status
admin	test@gmail.com	–	–	–
test_user	test1@gmail.com	–	–	–

13. Click **Details**.
14. Select update password from the **Required user actions** drop-down.
15. Click **Save**.

This user is added to your Keycloak account.

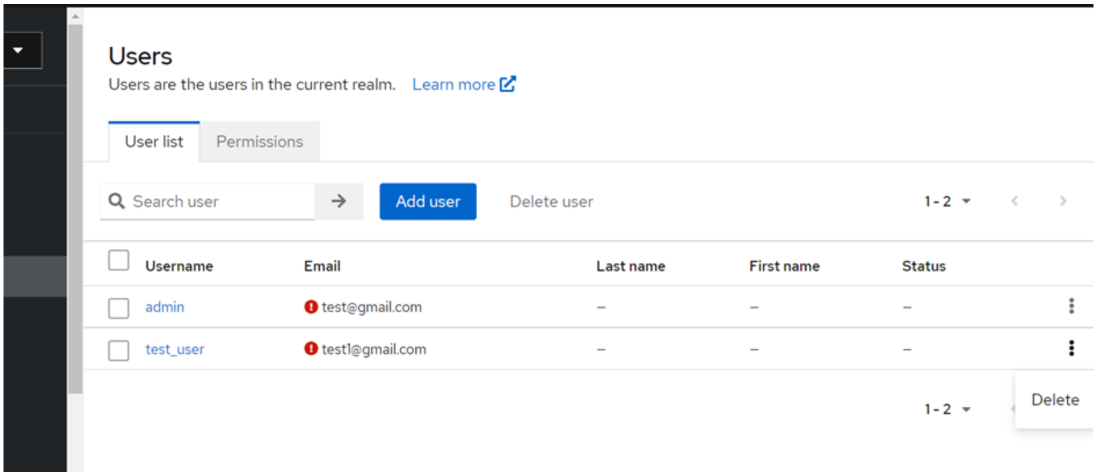
Deleting the Existing Users

To delete a user:

1. In the Keycloak console, click **Users**.

   The following screen appears.

   Figure 14 : Users list



Users

Users are the users in the current realm.

Username	Email	Last name	First name	Status
admin	test@gmail.com	–	–	–
test_user	test1@gmail.com	–	–	–

2. Click the **action** menu (three dots) next to the user that you want to remove.
3. Click **Delete**.

   The selected user is deleted.

Configuring Okta IDP for SSO

This section is intended for the IT administrator of your organization. The IT administrator must configure Okta IDP for SSO and integrate it with the Threat Control System application.

The following topics are covered:

Registering a New Application in Okta 63
Adding a New User and Setting the Authentication Policy 67
Integrating Okta with Threat Control System 71

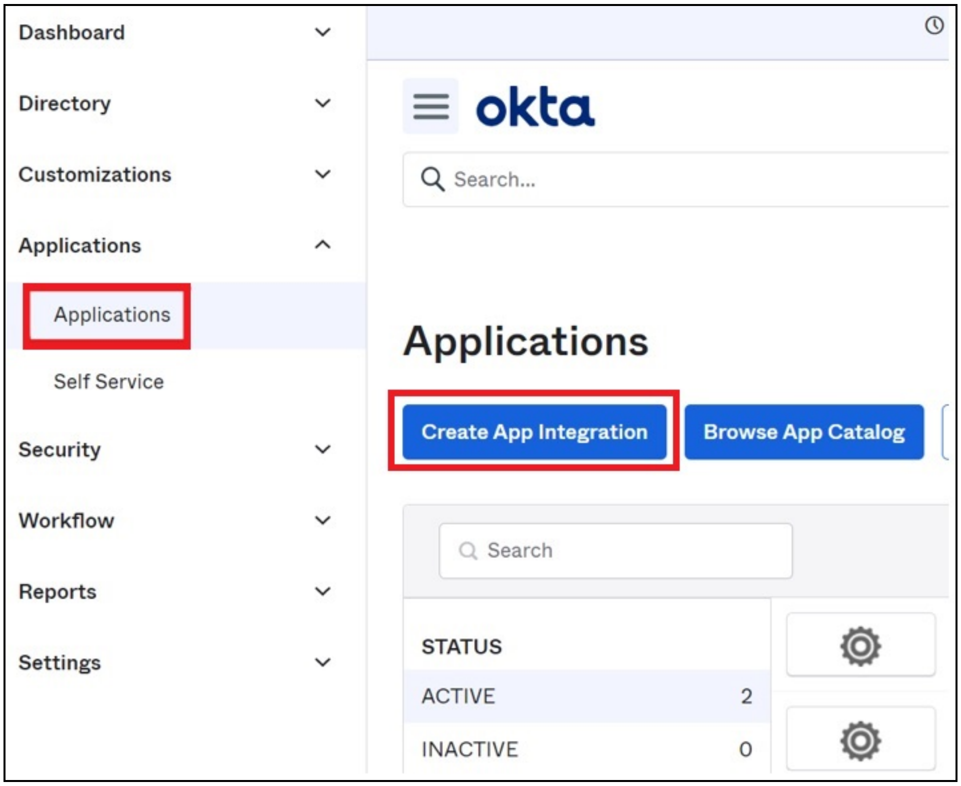
Registering a New Application in Okta

To authenticate users through Okta IDP, the organization must register a new application in Okta.

To register an application:

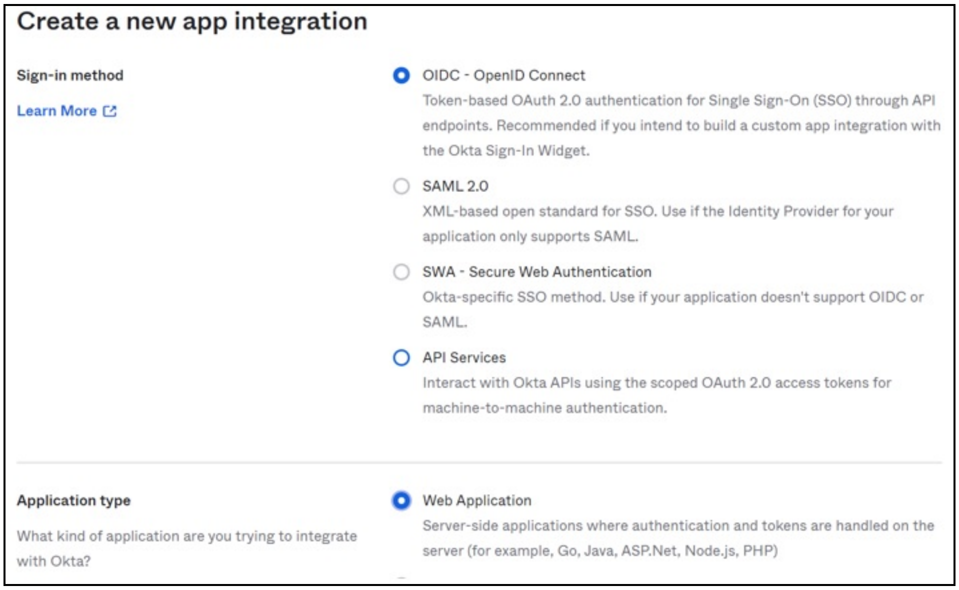
1. Go to https://developer.okta.com/login.
2. Click the **Hamburger** menu and navigate to **Applications > Applications**.

Figure 15 : Create App Integration



3. Click the **Create App Integration** button to create a new application.
4. Select the **OIDC - OpenID Connect** option as a Sign-in method and then select the **Web Application** option as the Application type. Click **Next**.

Figure 16 : OIDC - OpenID Connect



Create a new app integration

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

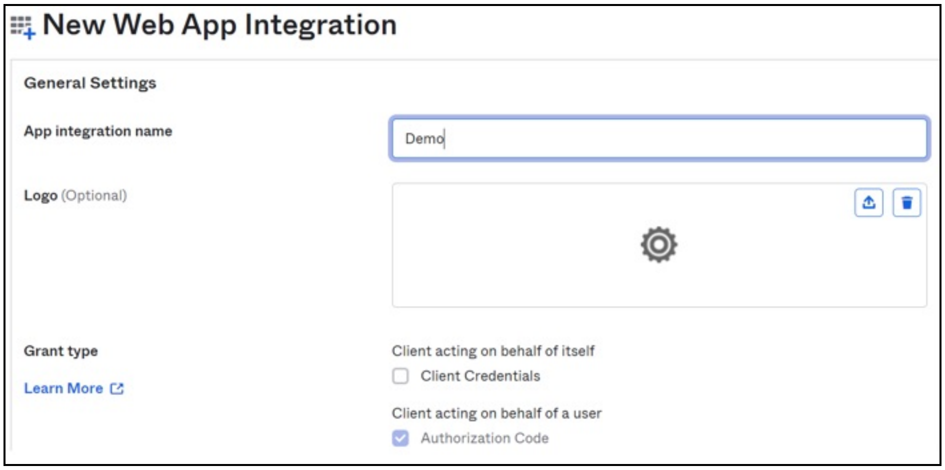
What kind of application are you trying to integrate with Okta?

● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

NOTE: You must select **OIDC - OpenID Connect** to enable Single Sign-On (SSO) through API.

5. Enter an application name. (Example: Demo).

Figure 17 : Web Application Integration



New Web App Integration

General Settings

App integration name: Demo

Logo (Optional)

Grant type

Learn More

Client acting on behalf of itself
☐ Client Credentials

Client acting on behalf of a user
☑ Authorization Code

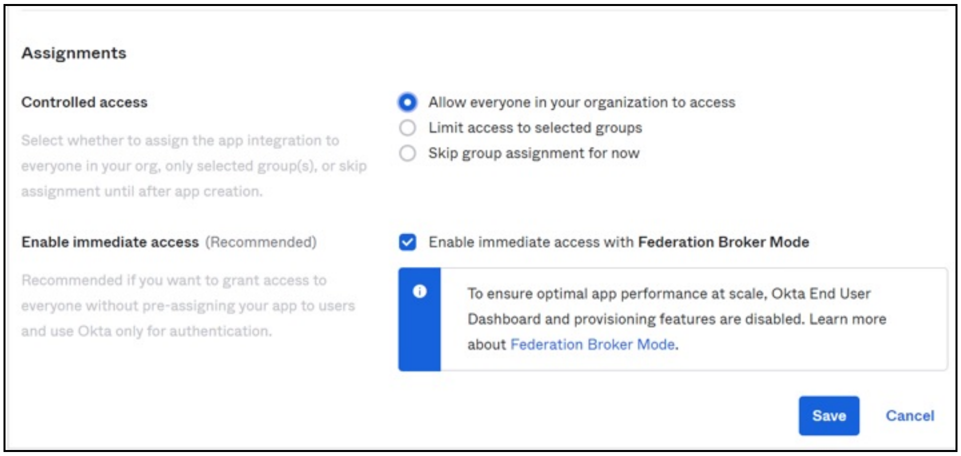
6. Select an access **Grant type**. The following options are available:

- **Client acting on behalf of itself**
- **Client acting on behalf of a user**.

  Client acting on behalf of a user is selected by default.

7. Select an access policy under **Controlled access**. (Example: Allow everyone in your organization to access). This option is selected by default. Click **Save**.

   Figure 18 : Controlled access



Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

● Allow everyone in your organization to access
○ Limit access to selected groups
○ Skip group assignment for now

Enable immediate access (Recommended)

Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

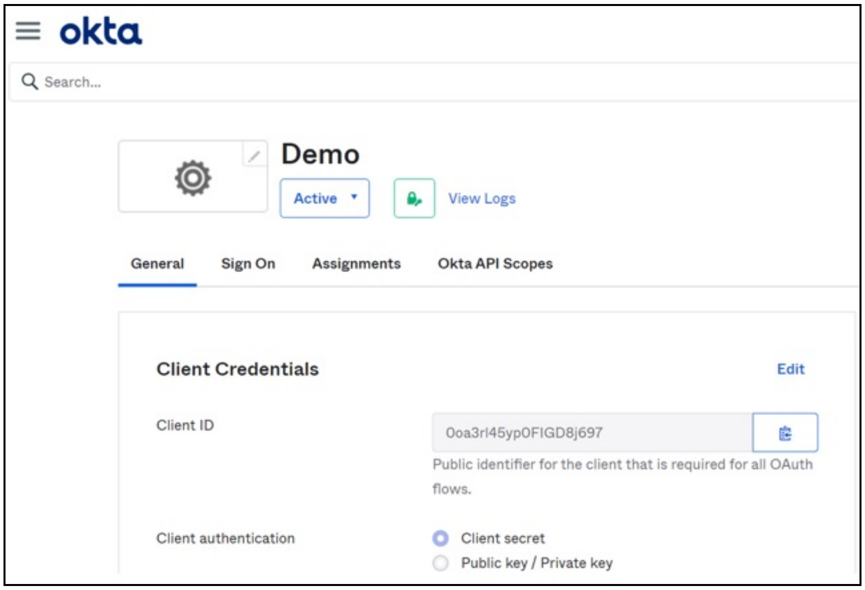
☑ Enable immediate access with **Federation Broker Mode**

To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about Federation Broker Mode.

8. Select **Enable immediate access with Federation Broker Mode** under **Enable immediate access**. This option is selected by default.

   The new application is registered successfully with Client ID and Client Secret. These keys will be used while adding a new organization to Threat Control System.

Figure 19 : General settings



Client Credentials

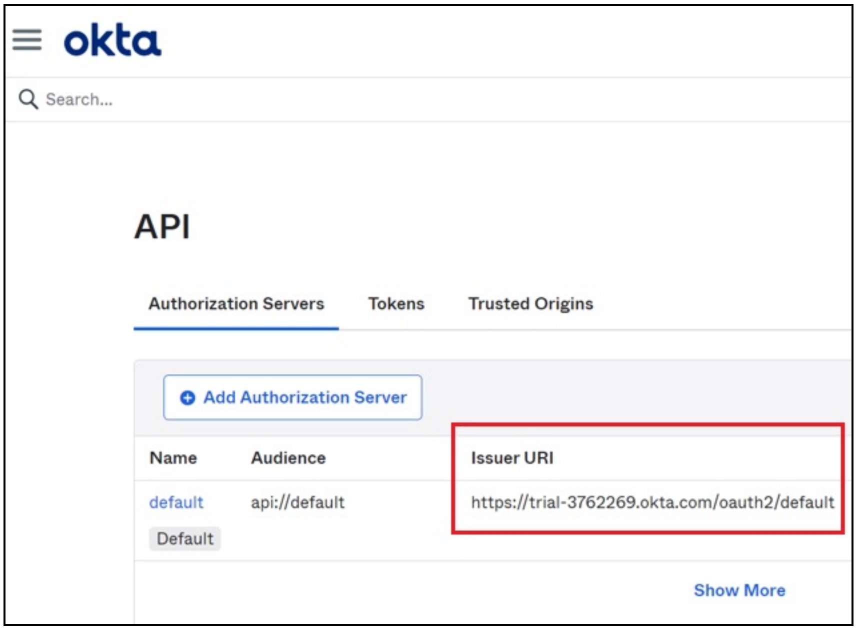
Client ID: 0oa3rl45yp0FIGD8j697

Public identifier for the client that is required for all OAuth flows.

Client authentication: ● Client secret ○ Public key / Private key

9. Click the **Hamburger** menu and navigate to **Security > API**.
10. On the **Authorization Servers** tab, a default Authentication Server is provided to authenticate the user requests. Click **Next**.

Figure 20 : Authorization Servers



Name	Audience	Issuer URI
default Default	api://default	https://trial-3762269.okta.com/oauth2/default

Save this Authentication Server URL or Issuer URI as it will be required to add an identity provider (IDP) in Okta.

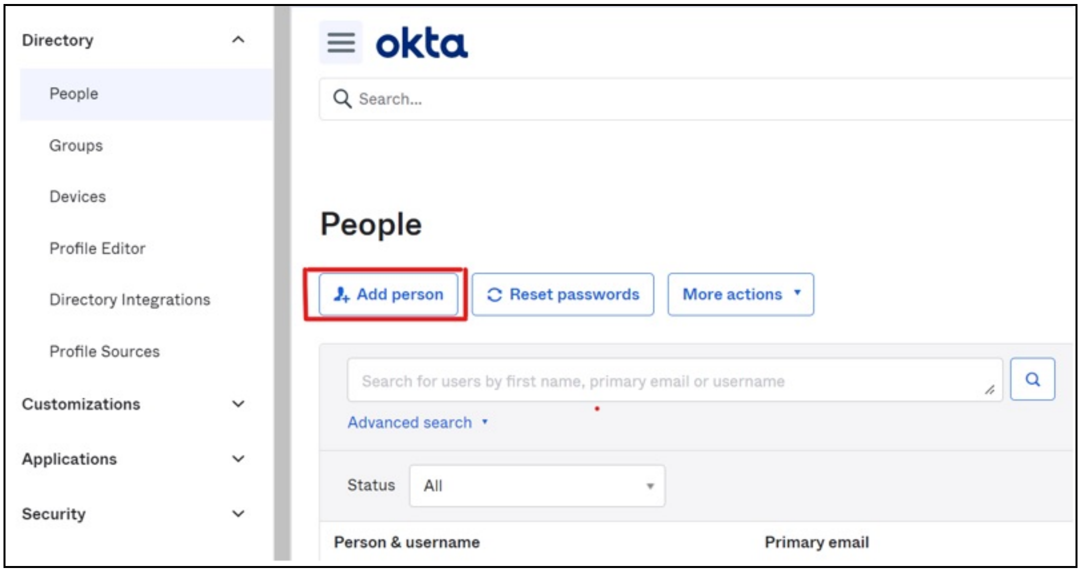
Adding a New User and Setting the Authentication Policy

After registering a new application in Okta, you must add a new user and set the authentication policy.

To add a user:

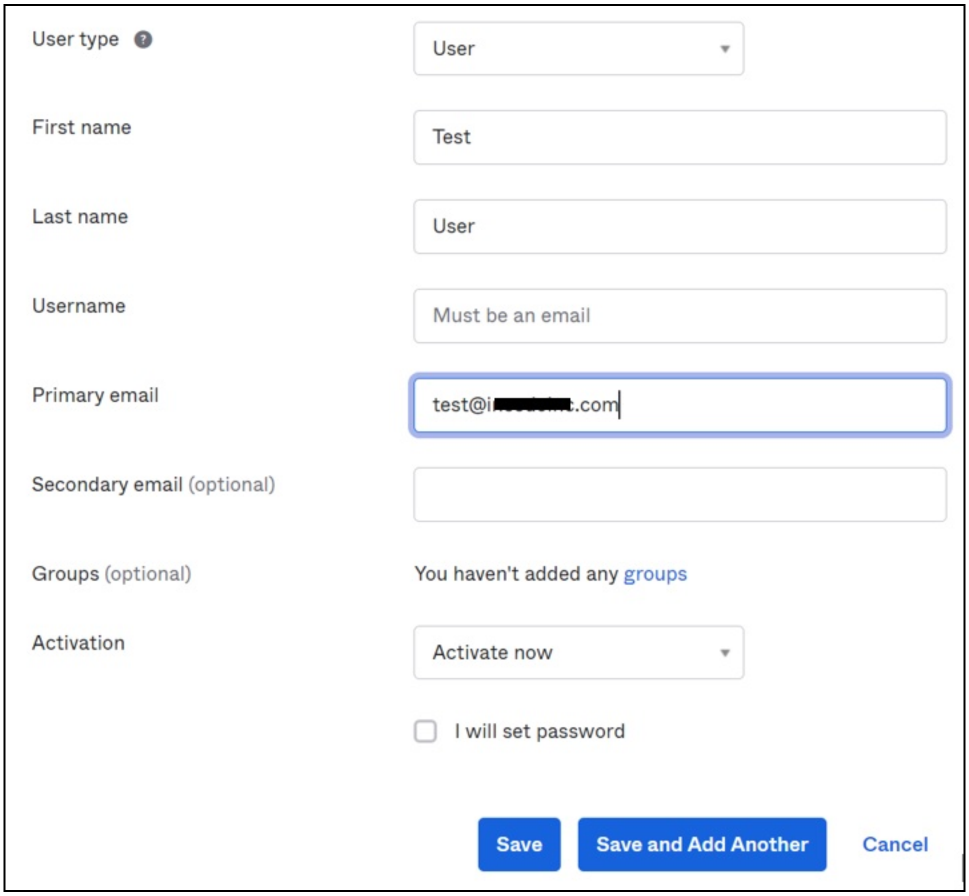
1. Click the **Hamburger** menu and navigate to **Directory > People**.

   Figure 21 : Add a person

2. Click the **Add person** button.
3. On the **Add person** screen, enter the user details.

Figure 22 : User Details



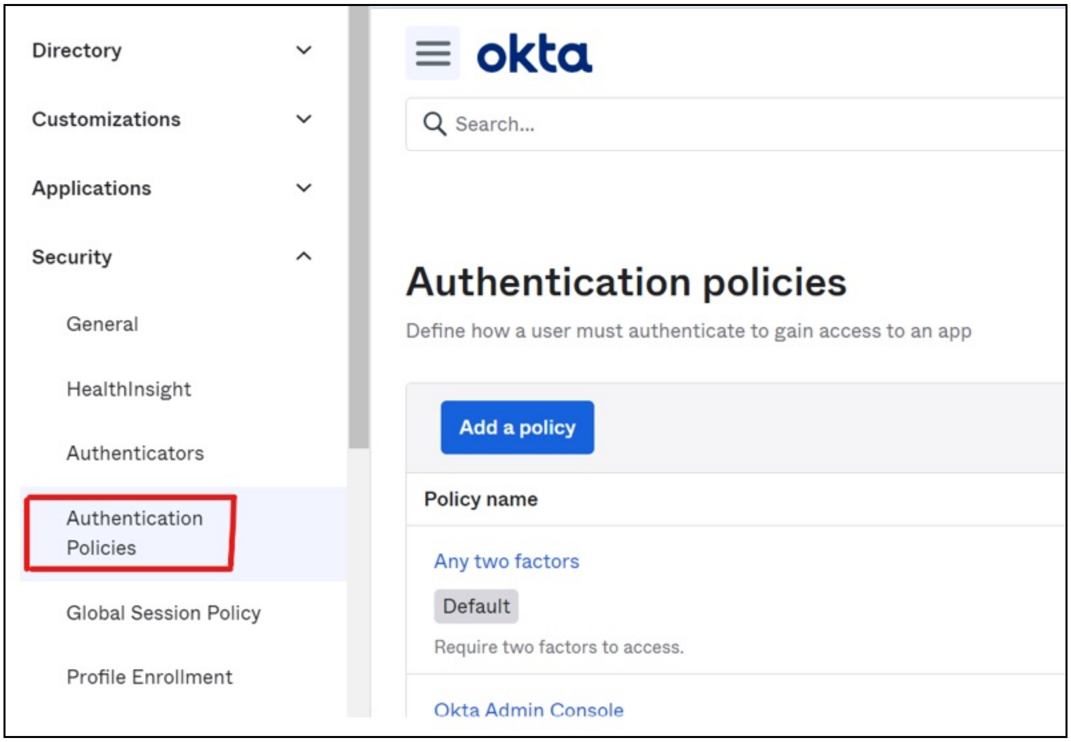
User type	User ▾
First name	Test
Last name	User
Username	Must be an email
Primary email	test@i[redacted].com
Secondary email (optional)	
Groups (optional)	You haven't added any groups
Activation	Activate now ▾
	□ I will set password

4. Click **Save**.

To set the authentication policy:

1. Click the **Hamburger** menu and navigate to **Security > Authentication Policy**.

   Figure 23 : Authentication Policy



Authentication policies

Define how a user must authenticate to gain access to an app

Policy name

Any two factors

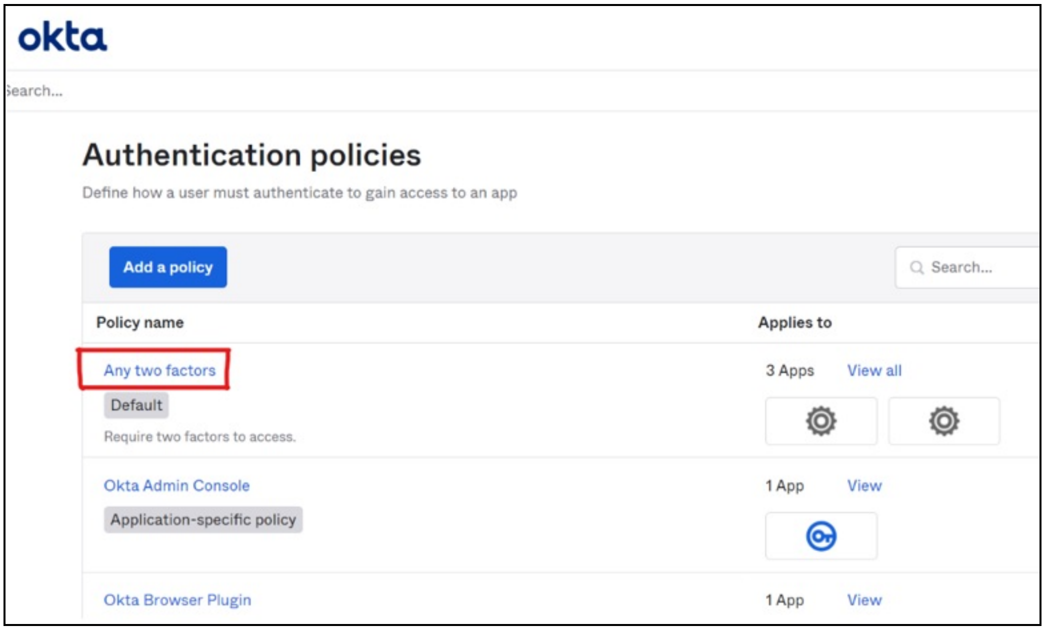
Default

Require two factors to access.

Okta Admin Console

2. By default, **Any two factors** policy is available for all the applications. This user will be authenticated using the 2-factor authentication. You can set the authentication policy as per your requirement.
3. Select the **Password Only** link to enable only password for user authentication.

Figure 24 : Any two factors



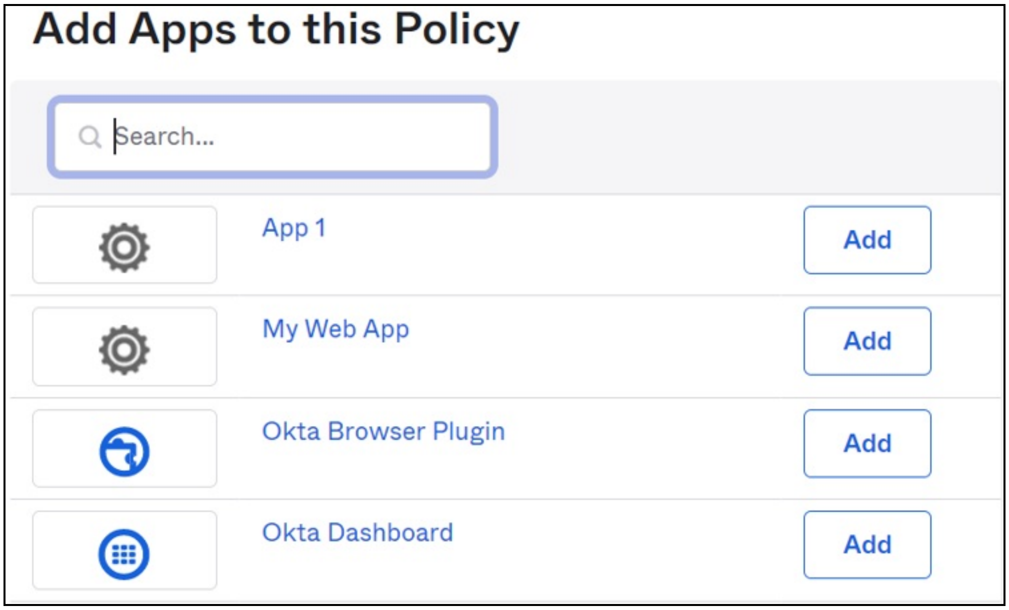
Authentication policies

Define how a user must authenticate to gain access to an app

Policy name	Applies to
Any two factors Default Require two factors to access.	3 Apps View all
Okta Admin Console Application-specific policy	1 App View
Okta Browser Plugin	1 App View

4. Click the **Applications** tab and click the **Add App** button to add the selected application to a policy.
5. Select the application to which you want to implement this Authentication Policy.

Figure 25 : Add apps to Policy



Add Apps to this Policy

App 1	Add
My Web App	Add
Okta Browser Plugin	Add
Okta Dashboard	Add

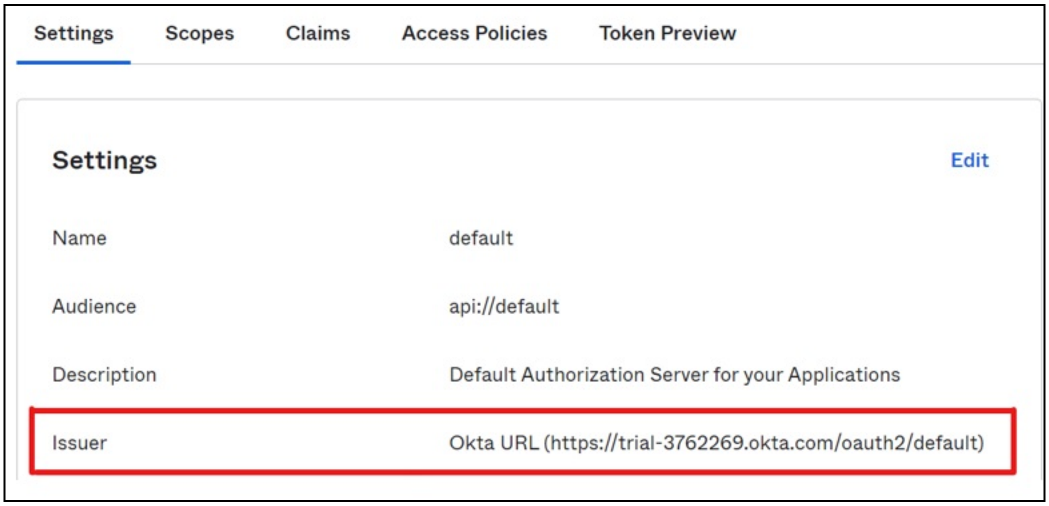
Integrating Okta with Threat Control System

To integrate the Okta keys with Threat Control System, the organization must keep the Client ID, Client Secret, and Issuer URI handy that were created in Registering a New Application in Okta.

To integrate the Okta keys:

1. Click the **Hamburger** menu and navigate to **Security > API**.
2. Click the **Authorization Servers** tab under API. Click Authorization Server that you created in Okta.

   Figure 26 : Issuer

   Settings

   Name default

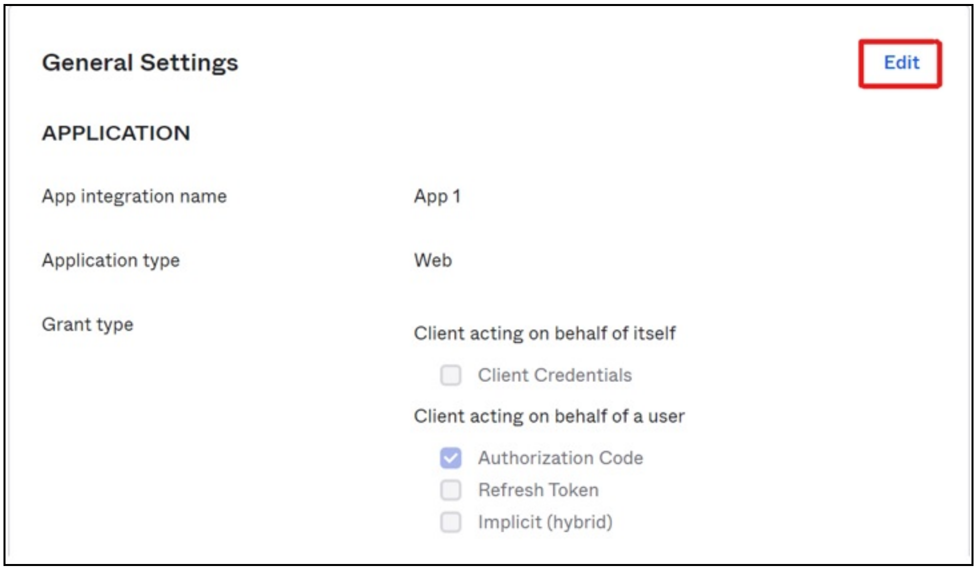
   Audience api://default

   Description Default Authorization Server for your Applications

   Issuer Okta URL (https://trial-3762269.okta.com/oauth2/default)

   The Authentication Server that you created is displayed in the list.
3. Navigate to your application.
4. Click the **Edit** option on the Settings screen.

Figure 27 : General Settings



General Settings

Edit

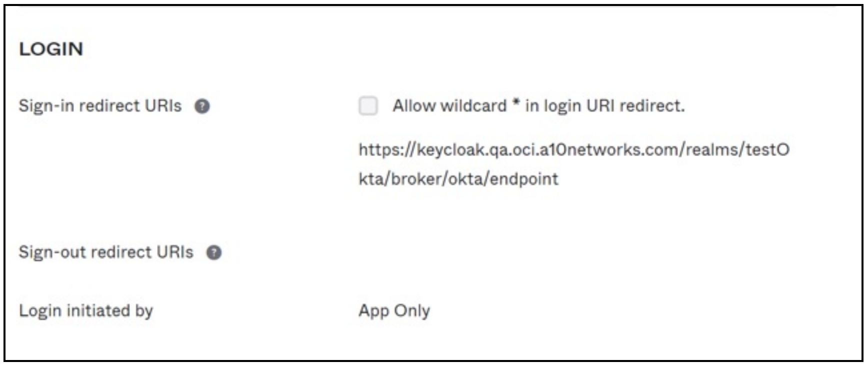
APPLICATION

App integration name	App 1
Application type	Web
Grant type	Client acting on behalf of itself □ Client Credentials Client acting on behalf of a user ☑ Authorization Code □ Refresh Token □ Implicit (hybrid)

5. Add the **Sign-in Redirect URI** in the following format: https://keycloak.a10networks.com/realms/{organizationname}/broker/Okta/endpoint.

   Ensure that you write the actual organization name in place of {organizationname}.

   Figure 28 : Organization onboarded with Keycloak



LOGIN

Sign-in redirect URIs	□ Allow wildcard * in login URI redirect. https://keycloak.qa.oci.a10networks.com/realms/testOkta/broker/okta/endpoint
Sign-out redirect URIs	
Login initiated by	App Only

Configuring Microsoft Azure IDP for SSO

This section is intended for the IT administrator of your organization. The IT administrator must configure Azure IDP for SSO and integrate it with the Threat Control System application.

The following topics are covered:

Configuring Access Token for Single Sign On (SSO) 73
Creating an Application Role to Assign to Groups 74
Assigning a Group to the Application in Microsoft Azure 75

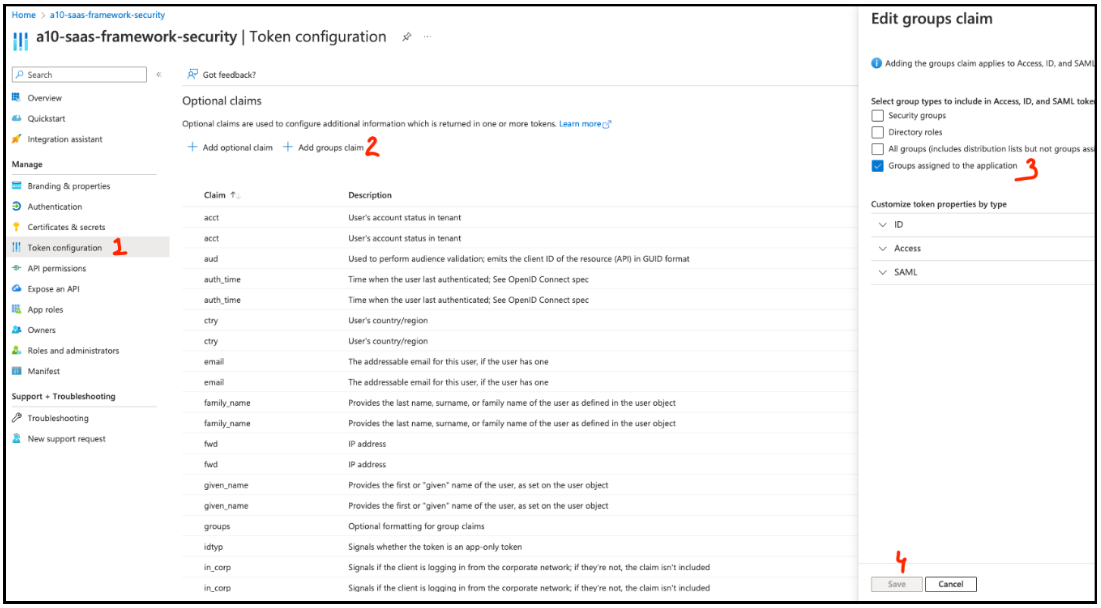
Configuring Access Token for Single Sign On (SSO)

To authenticate users through Single Sign On (SSO), the organization must create an access token.

To configure access token:

1. Log in to the administrator section of Threat Control System.

Figure 29 : Access Token



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description
acct	User's account status in tenant
acct	User's account status in tenant
aud	Used to perform audience validation; emits the client ID of the resource (API) in GUID format
auth_time	Time when the user last authenticated; See OpenID Connect spec
auth_time	Time when the user last authenticated; See OpenID Connect spec
ctry	User's country/region
ctry	User's country/region
email	The addressable email for this user, if the user has one
email	The addressable email for this user, if the user has one
family_name	Provides the last name, surname, or family name of the user as defined in the user object
family_name	Provides the last name, surname, or family name of the user as defined in the user object
fwd	IP address
fwd	IP address
given_name	Provides the first or "given" name of the user, as set on the user object
given_name	Provides the first or "given" name of the user, as set on the user object
groups	Optional formatting for group claims
idtyp	Signals whether the token is an app-only token
in_corp	Signals if the client is logging in from the corporate network; if they're not, the claim isn't included
in_corp	Signals if the client is logging in from the corporate network; if they're not, the claim isn't included

Edit groups claim

Adding the groups claim applies to Access, ID, and SAML

Select group types to include in Access, ID, and SAML toke

□ Security groups
□ Directory roles
□ All groups (includes distribution lists but not groups ass
☑ Groups assigned to the application

Customize token properties by type

- ID
- Access
- SAML

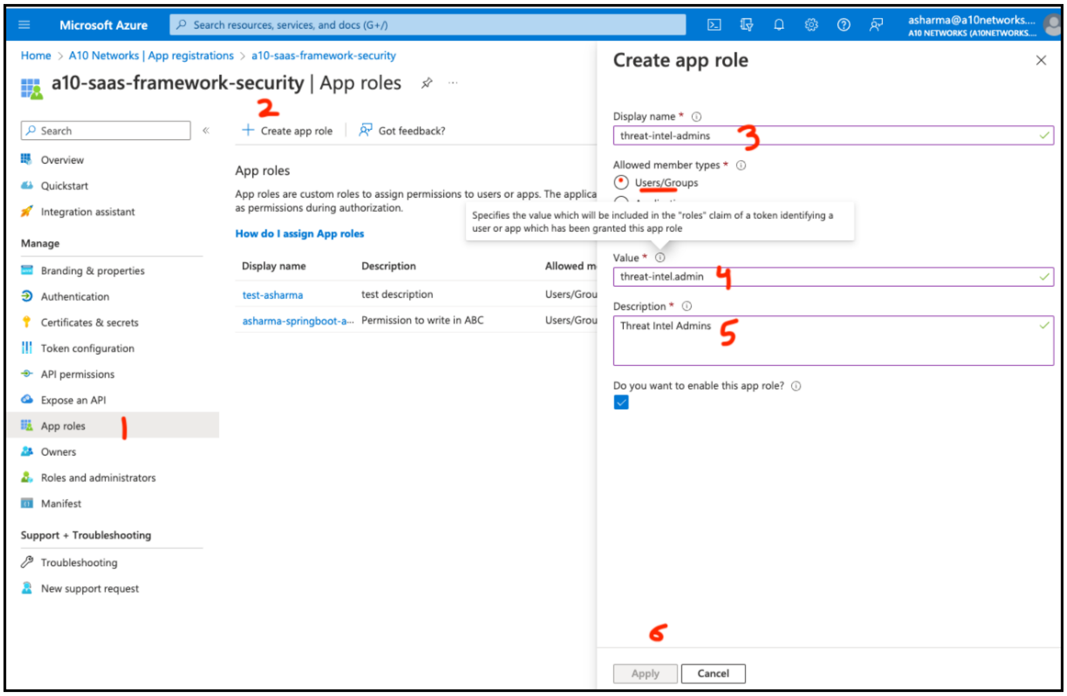
2. Navigate to **Token Configuration**, click **Add groups claim**, and then check **Groups assigned to the application**.
3. Deselect other options such as **Security groups**, **Directory roles**, and **All groups**, and then click **Save**.

Creating an Application Role to Assign to Groups

To create an application role:

1. Log in to the administrator section of Threat Control System.

   Figure 30 : Application Role



App roles

App roles are custom roles to assign permissions to users or apps. The applica as permissions during authorization.

Display name	Description	Allowed m
test-asharma	test description	Users/Grou
asharma-springboot-a...	Permission to write in ABC	Users/Grou

Display name * : threat-intel-admins

Allowed member types * : ● Users/Groups

Specifies the value which will be included in the "roles" claim of a token identifying a user or app which has been granted this app role

Value * : threat-intel.admin

Description * : Threat Intel Admins

Do you want to enable this app role? ☑

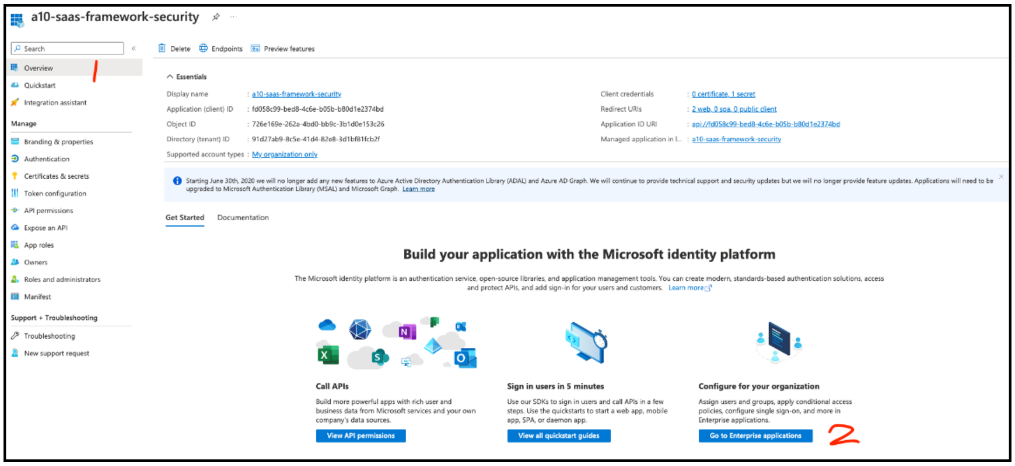
2. Navigate to **App roles** and click **Create app role**.
3. On the **Create app role** screen:
   - Enter a user/group name in the **Display name** field.
   - Select **Users/Groups**.
   - Enter a value to the admin user/group.
   - Enter a description about the user/group.
4. Select **Do you want to enable this app role?**
5. Click **Apply**.

Assigning a Group to the Application in Microsoft Azure

To assign a user/group to the application:

1. In the administrator section of Threat Control System, click the **Overview** option.

   Figure 31 : Overview



Display name : a10-saas-framework-security
Application (client) ID : fd058c99-bed8-4c6e-b05b-b80d1e2374bd
Object ID : 726e169e-262a-4bd0-bb9c-3b1d0e153c26
Directory (tenant) ID : 91d27ab9-8c5e-41d4-82e8-3d1bf81fcb2f
Supported account types : My organization only

Client credentials : 0 certificate, 1 secret
Redirect URIs : 2 web, 0 spa, 0 public client
Application ID URI : api://fd058c99-bed8-4c6e-b05b-b80d1e2374bd
Managed application in l... : a10-saas-framework-security

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

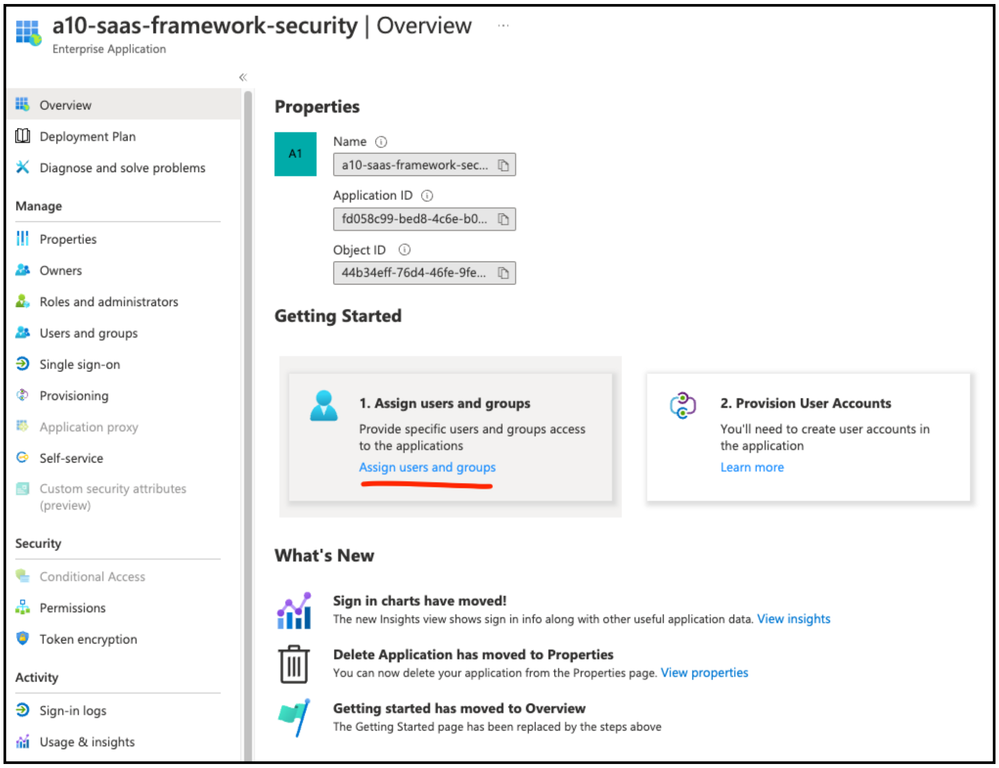
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Configure for your organization

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

2. Under **Build your application with the Microsoft identity platform**, click **Go to Enterprise application**.

Figure 32 : Assign users and groups



a10-saas-framework-security | Overview ...
Enterprise Application

«

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights

Properties

A1

Name ⓘ
a10-saas-framework-sec...

Application ID ⓘ
fd058c99-bed8-4c6e-b0...

Object ID ⓘ
44b34eff-76d4-46fe-9fe...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Provision User Accounts
You'll need to create user accounts in the application
Learn more

What's New

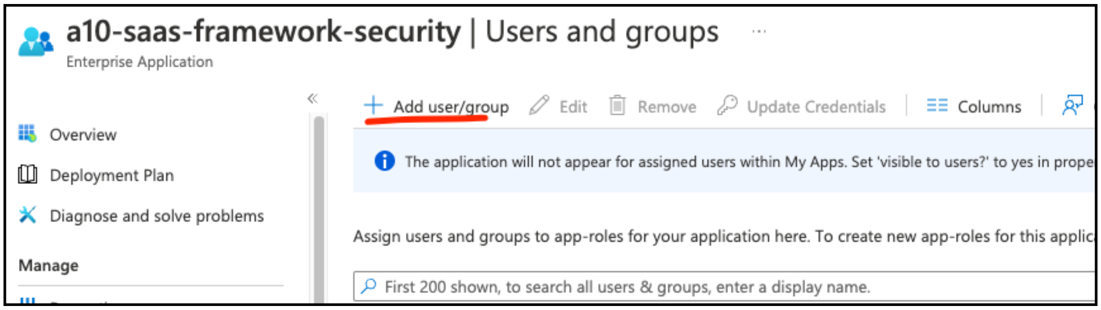
Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

3. Click **Assign users and groups**.

Figure 33 : Add user/group



a10-saas-framework-security | Users and groups ...
Enterprise Application

«

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

+ Add user/group ✎ Edit 🗑 Remove 🔑 Update Credentials ☰ Columns

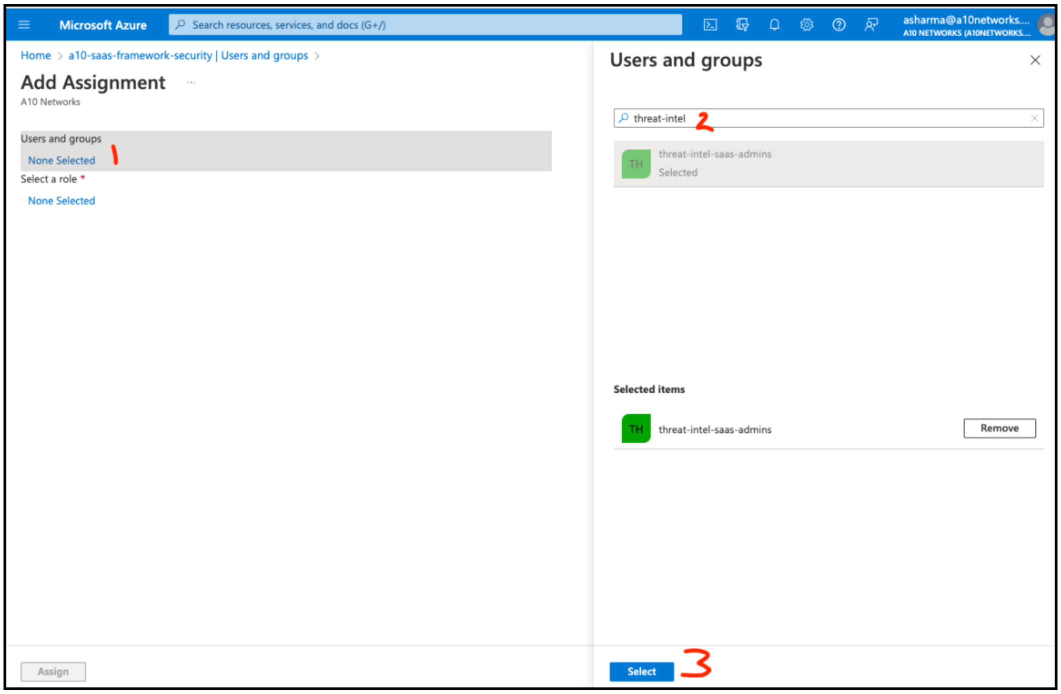
ⓘ The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in prope

Assign users and groups to app-roles for your application here. To create new app-roles for this applic

First 200 shown, to search all users & groups, enter a display name.

4. Click **Add user/group**.

Figure 34 : Assign users/groups


Microsoft Azure
Search resources, services, and docs (G+/)
asharma@a10networks....
A10 NETWORKS (A10NETWORKS...
Home > a10-saas-framework-security | Users and groups >
Add Assignment
A10 Networks
1
2
3
Users and groups
Selected items
Remove
Assign
Select

Users and groups: None Selected

Select a role *: None Selected

Users and groups search: threat-intel

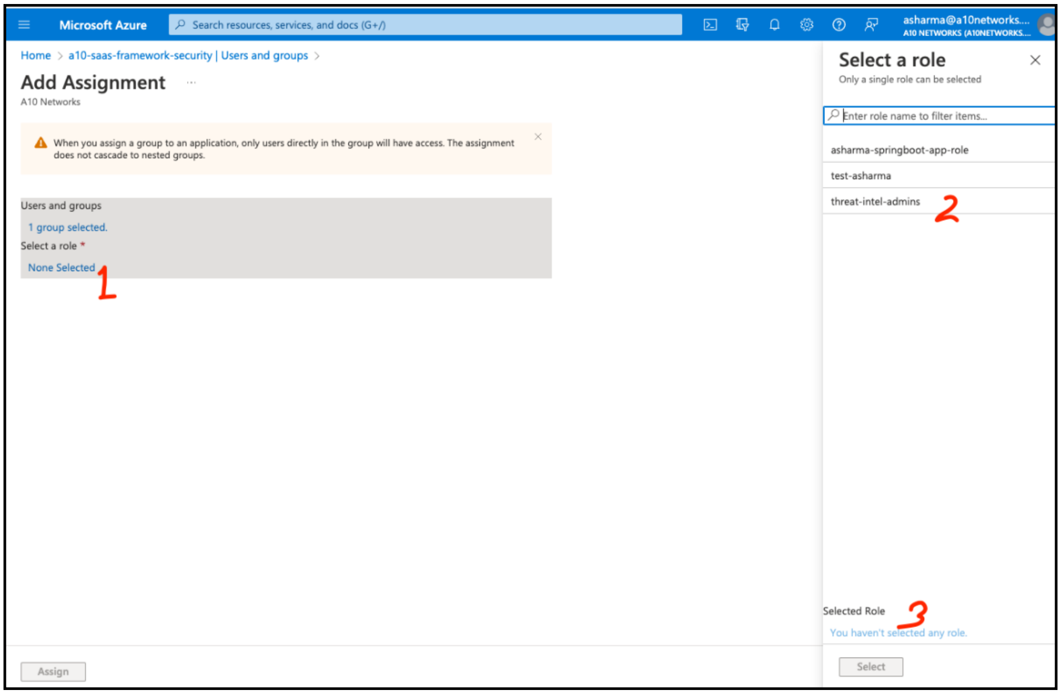
TH threat-intel-saas-admins: Selected

Selected items: TH threat-intel-saas-admins

5. Select **Users and groups**. Under Users and groups, select the group that you want to assign.
6. Click **Select**.

   The selected group will appear in the Users and groups list.

Figure 35 : Users/Groups Assigned


Microsoft Azure
Search resources, services, and docs (G+/)
asharma@a10networks....
A10 NETWORKS (A10NETWORKS....
Home > a10-saas-framework-security | Users and groups >
1
2
3
Assign
Select

Add Assignment

A10 Networks

When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

Users and groups

1 group selected.

Select a role *

None Selected

Select a role

Only a single role can be selected

Enter role name to filter items...

- asharma-springboot-app-role
- test-asharma
- threat-intel-admins

Selected Role

You haven't selected any role.

7. Assign the selected role to the group.

   When the access token of an organization is created, the following information is created.

   - IDP URL
   - Secret Key
   - App Key

   This information is required to configure Azure IDP.