



Platform User Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

Copyright © 2023 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

All other trademarks mentioned in this document are the property of their respective owners.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface.....	ix
Revision History.....	ix
About the Documentation.....	ix
Audience.....	ix
Text Conventions.....	ix
Chapter 1. Overview.....	10
Chapter 2. Configuring Authentication Settings	11
Configuring the LDAP Authentication.....	11
Configuring the TACACS Authentication.....	19
Enabling a TACACS Server for Authentication.....	24
Disabling a TACACS Server for Authentication.....	25
Deleting a TACACS Server.....	26
Configuring the RADIUS Configuration.....	27
Enabling a RADIUS Server for Authentication.....	34
Disabling a RADIUS Server for Authentication	34
Deleting a RADIUS Server	35
Configuring Single Sign On Settings with AppViewX.....	36
Security Assertion Markup Language.....	40
OpenID Connect- Overview.....	83
Configuring the IP Restrictions.....	105
Enabling a IP Restriction Rule	110
Disabling an IP Restriction Rule	111
Deleting an IP Restriction Rule	112
Configuring Authentication Settings.....	113
Configuring the MFA Settings.....	118
MFA Settings for User Profile.....	121
Logging in using MFA:.....	123

Chapter 3. Configuring Role and Resource-Based Access Control	127
Overview.....	127
Managing Users.....	128
Creating a User.....	129
Modifying a User.....	132
Importing a User.....	135
Enabling a User.....	136
Disabling a User.....	137
Deleting a User.....	138
Service Accounts.....	139
Client Credentials Grant Type.....	140
Managing Service Account.....	140
Configuring OAuth Settings.....	141
OAuth.....	145
OAuth Workflow	146
Managing User Groups.....	148
Creating a User Group.....	148
Cloning a User Group.....	150
Modifying a User Group.....	152
Enabling a User Group.....	154
Disabling a User Group.....	155
Deleting a User Group.....	156
Managing Roles.....	157
Creating a Role.....	158
Cloning a Role.....	160
Modifying a Role.....	162
Enabling a Role.....	163
Disabling a Role.....	164
Deleting a Role.....	166

RBAC Quick Configuration	167
Authentication.....	167
Resource.....	210
Role.....	225
User Group.....	237
Chapter 4. Configuring Privileged Access Management.....	253
Overview.....	253
AppViewX.....	255
CyberArk.....	257
Thycotic.....	259
Steps for Integration.....	260
HashiCorp.....	261
Linking Credentials in AppViewX from Hashicorp Vault.....	262
Chapter 5. Configuring General Settings.....	264
Configuring the SMTP Settings.....	264
Configuring the SMTP Settings for Google.....	264
Configuring the SMTP Settings for Microsoft	277
Managing Proxy Settings.....	298
Setting the Cryptographic Policy.....	301
Enabling Dashboard View for the User.....	304
Managing the Login Configuration.....	307
Restricting the Number of User Sessions.....	307
Restricting the Number of Login Attempts.....	309
Managing User Inactivity.....	313
Chapter 6. Managing Logs.....	316
Overview.....	316
Viewing Logs.....	317
Viewing All Logs.....	317
Viewing ADC Logs.....	319

Viewing AppViewX Logs.....	321
Viewing Audit Logs.....	323
Viewing Certificate Logs.....	325
Viewing Self-Audit Logs.....	327
Viewing SSH Logs.....	329
Viewing Syslog Logs.....	331
Viewing Workflow Logs.....	333
Setting the Record Count Preference for Logs.....	335
Searching for Logs.....	336
Based on a Timestamp.....	336
Based on the Values Recorded for each Log.....	337
Forwarding Logs.....	338
Configuring Server Inventory Settings.....	338
Configuring Forwarding Settings.....	343
Exporting Logs.....	345
Purging Logs.....	345
Chapter 7. HSM Integration for AppViewX.....	349
Overview.....	349
Utimaco.....	349
Integrating the Utimaco HSM with the AppViewX	350
Fortanix.....	354
Integrating the Fortanix HSM with the AppViewX.....	354
Thales DPoD.....	357
Integrating the Thales DPoD HSM with the AppViewX.....	357
Thales GPN.....	363
Installing the Luna Client.....	363
Integrating the Thales GPN HSM with the AppViewX.....	363
Chapter 8. Managing Alerts.....	370
Overview.....	370

Viewing Existing Alerts.....	371
Viewing All Alerts.....	371
Viewing AppViewX Alerts.....	373
Viewing Certificate Alerts.....	376
Viewing SSH Alerts.....	378
Viewing Syslog Alerts.....	379
Setting the Record Count Preference for Viewing Alerts.....	381
Configuring Alerts.....	381
Configuring ADC Alerts.....	382
Configuring AppViewX Alerts.....	387
Configuring Certificate Alerts.....	390
Configuring SSH Alerts.....	394
Configuring Syslog Alerts.....	398
Editing Alerts.....	403
Deleting Alerts.....	403
Searching for Alerts.....	404
Based on a Timestamp.....	404
Based on the Values Recorded for each Alert.....	406
Purging Alerts.....	406
Chapter 9. Managing Licenses.....	410
Overview.....	410
Upgrading Licenses.....	410
Viewing Licensing Details.....	412
Chapter 10. Customizing the AppViewX User Interface.....	415
Overview.....	415
Customizing the Email Attachment Representation.....	415
Customizing the Login Screen.....	419
Customizing the Logo.....	422
Customizing the Screen Header.....	426

Chapter 11. Glossary.....	432

Preface

Revision History

Revision	Description	Date
3.0	Updated version of document for Release 2022.1.0 FP2 Beta	November 2022
2.0	Updated version of document for Release 2022.1.0 FP1	September 2022
1.0	Initial Release of AppViewX_v2022.1.0 Platform.	June 2022

About the Documentation

The AppViewX Platform is a module that lets you enable general configuration settings such as authentication, authorization, and integration of external services like log forwarding, HSM integration, SMTP configuration, and so on. These general configuration settings are applicable to all AppViewX subsystems such as ADC, CERT+, Security+, Visual Workflow, and so on.

Audience

This guide is intended for CISO, PKI Security, and Application Teams.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter.

Chapter 1: Overview

The AppViewX Platform is a module that lets you enable general configuration settings such as authentication, authorization, and integration of external services like log forwarding, HSM integration, SMTP configuration, and so on. These general configuration settings are applicable to all AppViewX subsystems such as ADC, CERT+, Security+, Visual Workflow, and so on.

The Platform User Guide documents these general configuration settings.

Platform components common to all subsystems are shown in the image below:



Chapter 2: Configuring Authentication Settings

- [Configuring the LDAP Authentication](#)
- [Configuring the TACACS Authentication](#)
- [Configuring the RADIUS Configuration](#)
- [Configuring Single Sign On Settings with AppViewX](#)
- [Configuring the IP Restrictions](#)
- [Configuring Authentication Settings](#)
- [Configuring the MFA Settings](#)

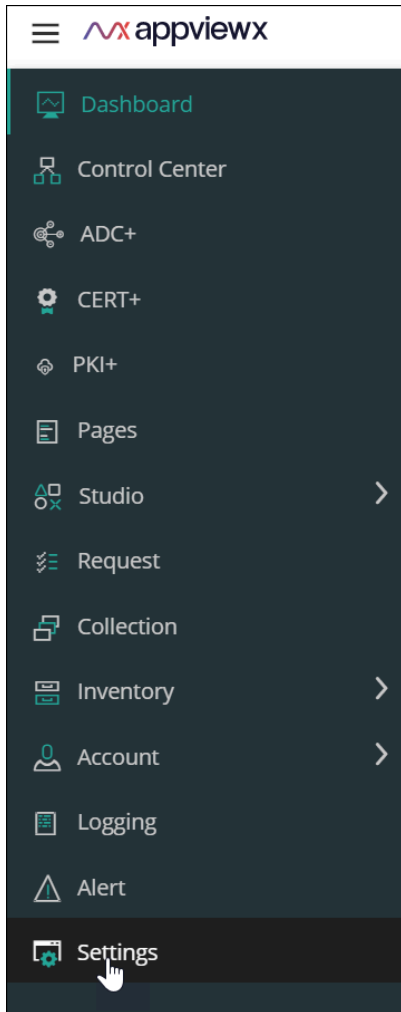
Configuring the LDAP Authentication

The Lightweight Directory Access Protocol (LDAP) is an authentication protocol to validate a user's credentials entered in an application, against the credentials stored in the Active Directory database.

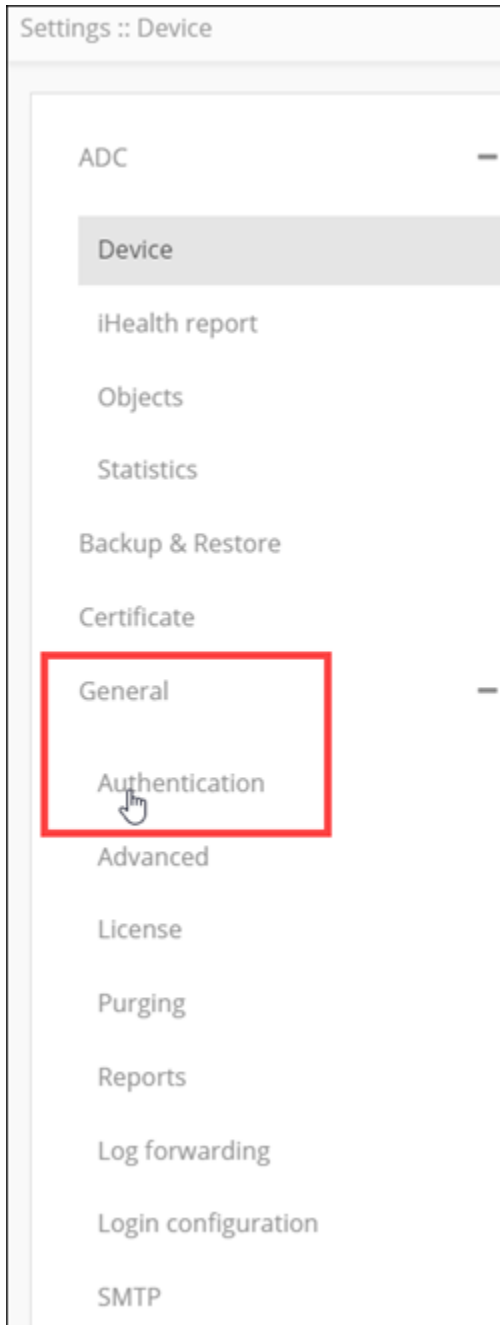
AppViewX integrates with the Active Directory and Open LDAP for authentication of external users. It also enables configuring multiple servers in the event that users belong to multiple domains.

To configure the LDAP authentication:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

Settings :: Authentication

Quick config 0 Entries

ADC LDAP TACACS RADIUS SSO IP Restriction Authentication settings OAuth Settings

Device
Health report
Objects
Statistics
Backup & Restore
Certificate
General
Authentication
Advanced
License
Purging
Reports
Log forwarding
Login configuration
SMTP

General information

* Host

* Port

LDAPS ☒

Upload certificate [Browse](#)

Bind DN

Bind password

Data center

Authorization ☒

Enable Nested Groups ☒

LDAP Sync ☒

5. To configure the LDAP settings, in the **General Information** section, enter the following details (sample values are shown in the image below the table):

Field	Description
*Host	Host name (domain name) of the LDAP server.
*Port	Port number of the LDAP server. Note: This value is entered based on the port number used in your deployment. By default, port number 389 is used for a LDAP configuration and port number 636 is used for a LDAPS configuration.
LDAPS	The LDAPS protocol is used for secure communication between AppViewX and Active Directory/Open LDAP. To enable use of the LDAPS protocol, enable this toggle.
Upload Certificate	Note: This field is enabled only when the LDAPS is enabled. To upload a LDAP server certificate: - Click Browse Certificate. - Navigate to the location of the .pem certificate file.

Field	Description
	 Note: If the LDAP servers are load balanced with VIP, upload the root certificate of the LDAP server instead of the server certificate. c. Select the certificate to be uploaded and click Open. The selected certificate is uploaded.  Note: Only a single certificate can be uploaded for each server.
Bind DN	Username of the base authentication endpoint that will be used to connect to LDAP.
Bind password	Password of the base authentication endpoint that will be used to connect to LDAP.
Authentication	In addition to authentication, AppViewX also lets you perform user authorization against the LDAP server. To enable authorization along with authentication, turn on the toggle.  Note: If Authorization is not enabled, AppViewX will only carry out LDAP authentication for the given user.
LDAP Sync	To enable the use of the SSH module in AppViewX for SSH key discovery use case, turn on the toggle.
All * marked fields are mandatory.	

LDAP
TACACS
RADIUS
SAML
IP Restriction
Authentication settings

General information

* Host

gs-ldap-pe1.lab.appviewx.net

* Port

389

LDAPS

☐

Upload certificate

Browse

Bind DN

CN=Administrator,CN=Users,DC=testavx,DC=com

Bind password

.....

Authorization

☒

LDAP Sync

☐

6. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click **Test Connection**.



Note: You can test the connection of LDAPS only when you save all of the configuration details. Bind DN and Bind password details cannot be validated through a test connection.

7. The **User Search** section collects information to validate a user's presence in the Active Directory. In the **User Search** section, enter the following details (sample values are shown in the image below the table):

Field	Description
*User search base	Base directory where the user is present.

Field	Description
*Search filter	Criteria for searching for the user from the search base.
User return attribute	User information to be retrieved from the search base.  Note: This field is enabled only when the Authorization toggle (in the General Information section) is turned on.  Note: You can specify only User return attribute.
All * marked fields are mandatory.	

User search

* User search base

* Search filter

User return attribute

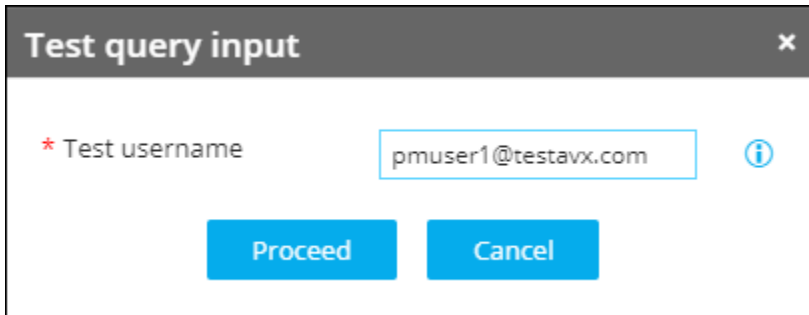
Add

User search base	Search filter	User return attribute	Actions
OU=Product Engineering,DC=testavx,DC=com	sAMAccountName{0}		Test query
OU=Product Management,DC=testavx,DC=com	sAMAccountName{0}		Test query



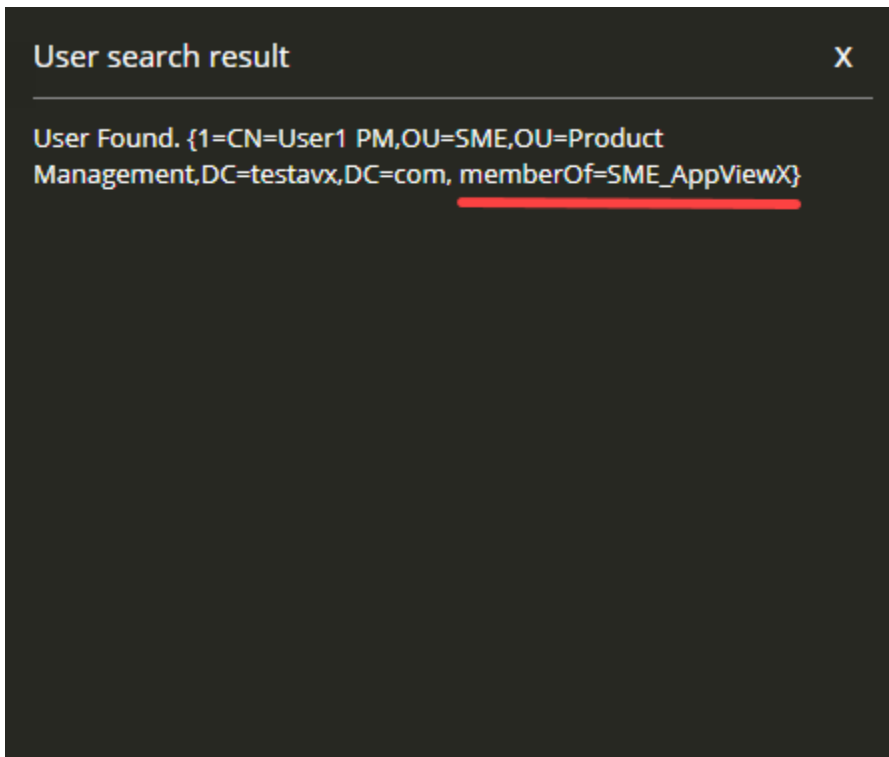
Note: You can now add multiple OUs in User search so that it checks multiple OUs to validate a user's presence in the Active Directory.

- For the given configuration, to check the user's presence, click **Test query**.
- In the **Test query input** dialog box, enter the **Test username**.



A dialog box titled "Test query input" with a close button (X) in the top right corner. It contains a label "* Test username" followed by a text input field containing "pmuser1@testavx.com". To the right of the input field is an information icon (i). At the bottom are two blue buttons: "Proceed" and "Cancel".

The output is displayed as shown in the image below:



A dark-themed dialog box titled "User search result" with a close button (X) in the top right corner. It displays the text "User Found. {1=CN=User1 PM,OU=SME,OU=Product Management,DC=testavx,DC=com, memberOf=SME_AppViewX}" where the "memberOf=SME_AppViewX" part is underlined in red.

10. To test which user group the user belongs to, in the **Group search** section, enter the following details:



Note: This section is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on.

Field	Description
*Group search base	Base directory where the user group is present.
*Search filter	Criteria to search the user group from the search base.
Group return attribute	User group information to be retrieved from the search base.

Field	Description
All * marked fields are mandatory.	



Note: You are allowed to check the query response for User search and Group search only when the connection is valid.



Note: Group search can be performed only if the customer's LDAP is of type Open LDAP. Microsoft Active Directory does not need group search configuration. For Open LDAP, group search needs to be configured mandatorily. The User return attribute in the User search section does not return the group membership details.

- After entering the above details, to test if the group search query thus configured works, click **Test Query**. For Open LDAP, when the user runs the test query for group search, the user search base details are passed to the group search test query and the group membership details for that user are returned.

- To save the LDAP settings, click **Save** or to reconfigure the settings, click **Reset**.

The LDAP authentication settings thus configured are saved and displayed in the table shown at the end of this screen:

Host	Bind DN	Group search base	Authorization	AD user groups	
ldap://gs-ldap-pe1.lab.appviewx.net:389	CN=Administrator,CN=Users,DC=testavx.DC=com	DC=testavx.DC=com	true	Fetch user groups	



Note: In the case of multiple LDAP servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

Configuring the TACACS Authentication

The Terminal Access Controller Access Control System (TACACS) authentication is used to validate users requesting remote access. AppViewX integrates with TACACS for authentication of external users.

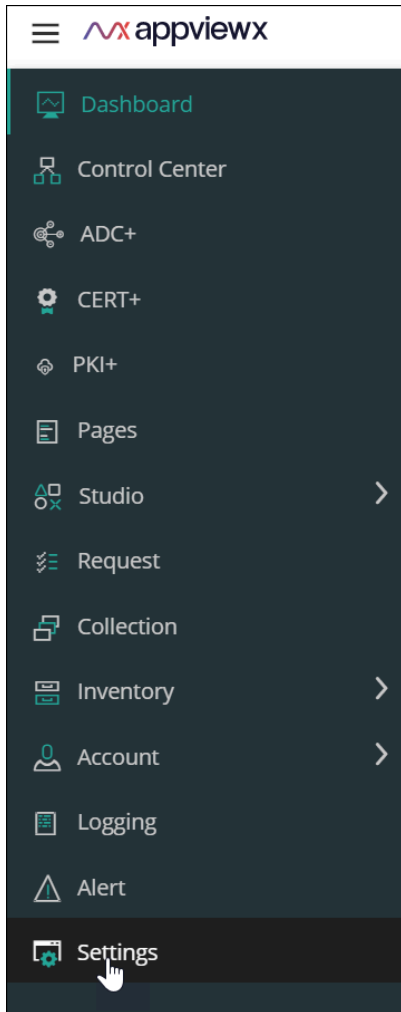
To configure the TACACS authentication:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the

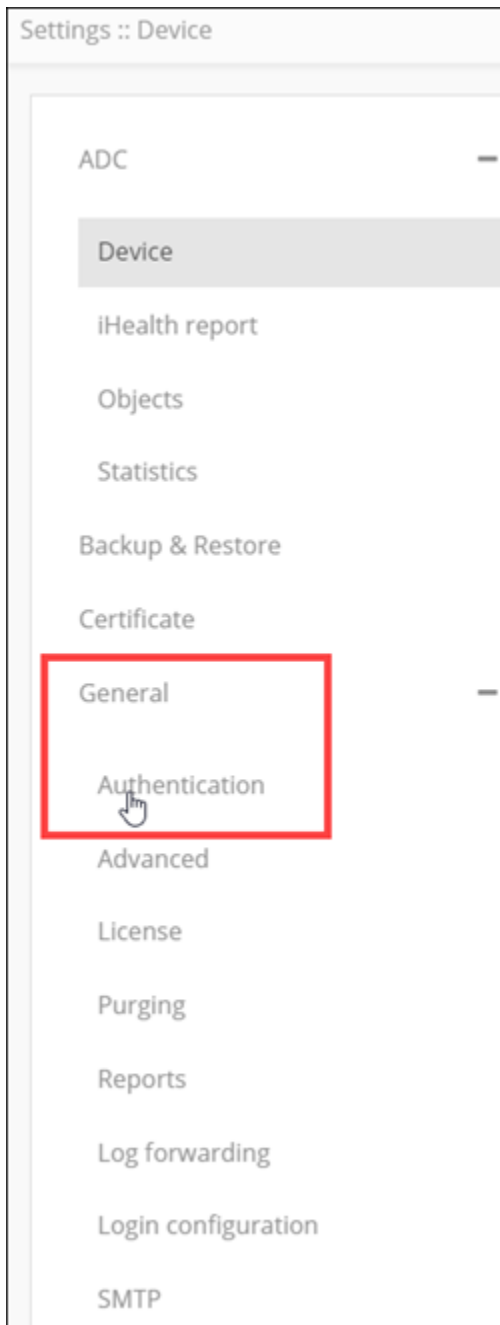


icon.

- From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

The screenshot shows the 'Settings :: Authentication' page with the 'General information' tab selected. The left sidebar lists various settings categories, with 'Authentication' highlighted. The main content area contains the following fields:

- Host:** A text input field.
- Port:** A text input field with the value '389'.
- LDAPS:** A checkbox that is checked.
- Upload certificate:** A button labeled 'Browse'.
- Bind DN:** A text input field with the value 'CN=admin,DC=example,DC=com'.
- Bind password:** A text input field.
- Data center:** A dropdown menu with the value 'dc1'.
- Authorization:** A checkbox that is checked.
- Enable Nested Groups:** A checkbox that is checked.
- LDAP Sync:** A checkbox that is checked.

5. To configure the **TACACS** authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.

The screenshot shows the 'Settings :: Authentication' page with the 'TACACS' tab selected. The left sidebar is the same as the previous screenshot. The main content area contains the following elements:

- Table:** A table with columns 'Server name', 'IP address', 'Port', and 'Status'. It currently shows 'No records found' and a 'Save' button.
- Form Fields:**
 - *Server name:** A text input field.
 - *IP address:** A text input field.
 - *Port:** A text input field.
 - *Secret key:** A text input field.
 - *Service:** A text input field.
 - *Protocol:** A text input field.
 - *Authorization attribute name:** A text input field.
- Buttons:** A 'Test connection' button and 'Add' and 'Reset' buttons at the bottom right.

6. Enter the following details (sample values are shown in the image below the table):

Field	Description
*Server name	Name of the TACACS server.
*IP address	IP address of the TACACS server.
*Port	Port number of the TACACS server.
All * marked fields are mandatory.	

* Server name	tacacs
* IP address	192.168.142.89
* Port	49
Test connection	

7. To test the connectivity between AppViewX and the IP address mentioned above, click **Test connection**.

8. Enter the following details (sample values are shown in the image below the table):

Field	Description
*Secret key	A unique key for authentication between the AppViewX server and the TACACS server.
*Service	Name of the service used by the user requested to be authorized. Specifying the service name is mandatory because it enables the TACACS+ server to behave according to the type of each authorization request. Commonly, the Point-to-Point Protocol (PPP) is used for authorization checks.
*Protocol	The protocol associated with the value specified in Service Name, which is a subset of the associated service being used for client authorization or system accounting Commonly, the Internet Protocol (IP) is used as the modifier with PPP to indicate the protocol layer for authorization check.
*Authorization Attribute Name	Attribute that will be returned from the TACACS server to authenticate and authorize the connection between the AppViewX server and the TACACS server.
All * marked fields are mandatory.	

* Secret key	
* Service	ppp
* Protocol	IP
* Authorization attribute name	role

9. To save the TACACS authentication settings, click **Add** or to reconfigure the settings, click **Reset**.

The TACACS authentication settings thus configured are saved and displayed in the table shown in the left half of the screen:

☐	Server name	IP address	Port	Status	
☐	tacacs	192.168.142.89	49	✓ Enabled	



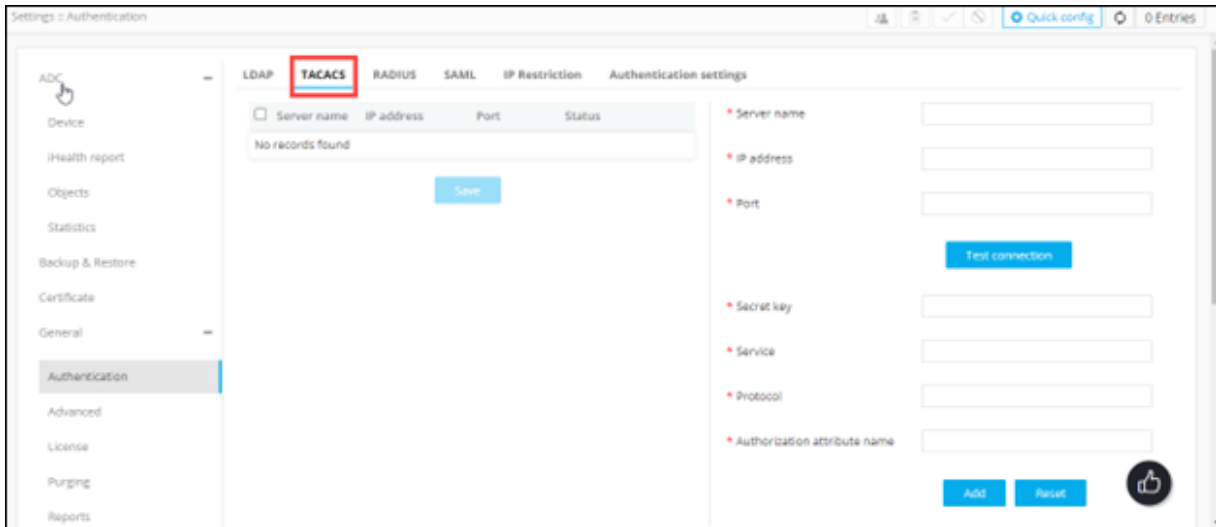
Note: In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- [Enabling a TACACS Server for Authentication](#)
- [Disabling a TACACS Server for Authentication](#)
- [Deleting a TACACS Server](#)

Enabling a TACACS Server for Authentication

To enable a TACAS server for authentication:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the TACACS authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



3. From the table displayed in the left half of the page, for the server you want to enable, select the check box corresponding to the server name.

☒	Server name	IP address	Port	Status	
☒	tacacs	192.168.142.89	49	Disabled	

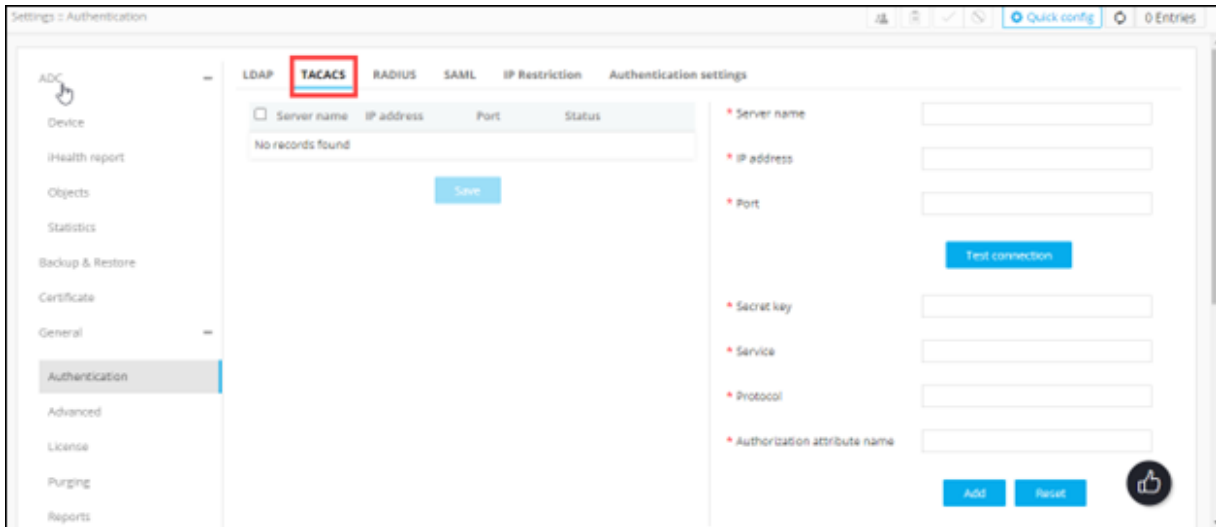


4. From the top-right corner of the page, click **Enable**.
5. In the **Confirmation message** dialog box, click **Proceed**.

Disabling a TACACS Server for Authentication

To disable a TACAS server for authentication:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the TACACS authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



- From the table displayed in the left half of the page, for the server you want to disable, select the check box corresponding to the server name.

☒	Server name	IP address	Port	Status	
☒	tacacs	192.168.142.89	49	Enabled	

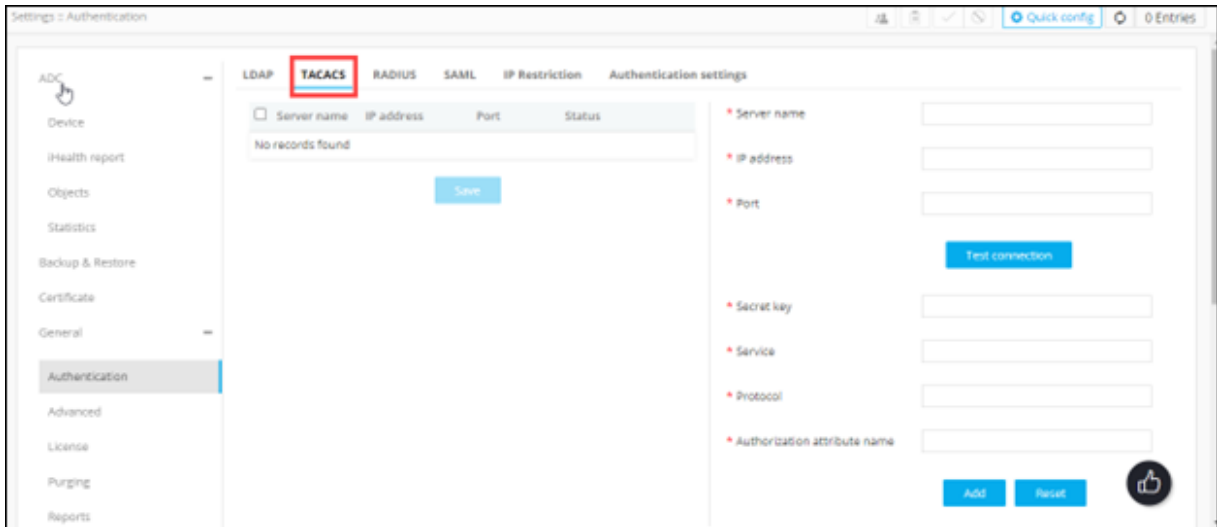


- From the top-right corner of the page, click **Disable**.
- In the **Confirmation message** dialog box, click **Proceed**.

Deleting a TACACS Server

To delete a TACAS server :

- Navigate to the **Settings :: Authentication** page.
- To configure the TACACS authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



3. From the table displayed in the left half of the page, for the server you want to delete, select the check box corresponding to the server name.

☒	Server name	IP address	Port	Status	
☒	tacacs	192.168.142.89	49	Enabled	



4. From the top-right corner of the page, click **Delete**.
5. In the **Confirmation message** dialog box, click **Proceed**.

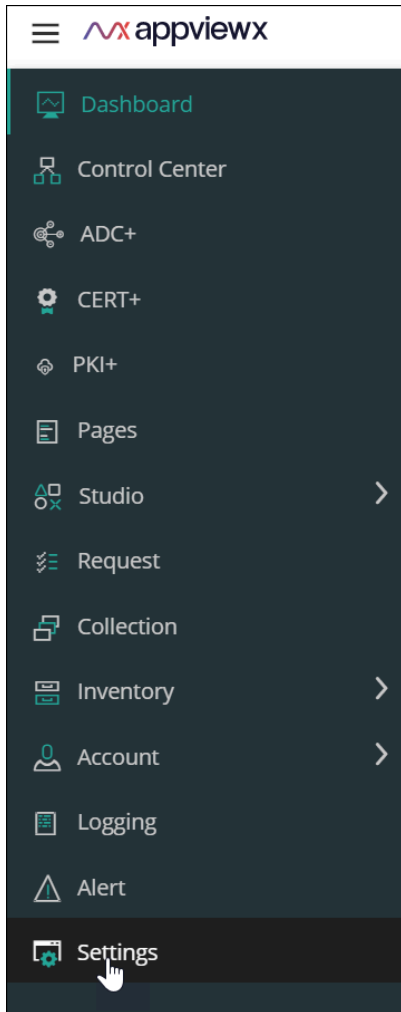
Configuring the RADIUS Configuration

The Remote Authentication Dial-In User Service (RADIUS) protocol is a networking protocol that provides centralized authentication, authorization, and accounting management.

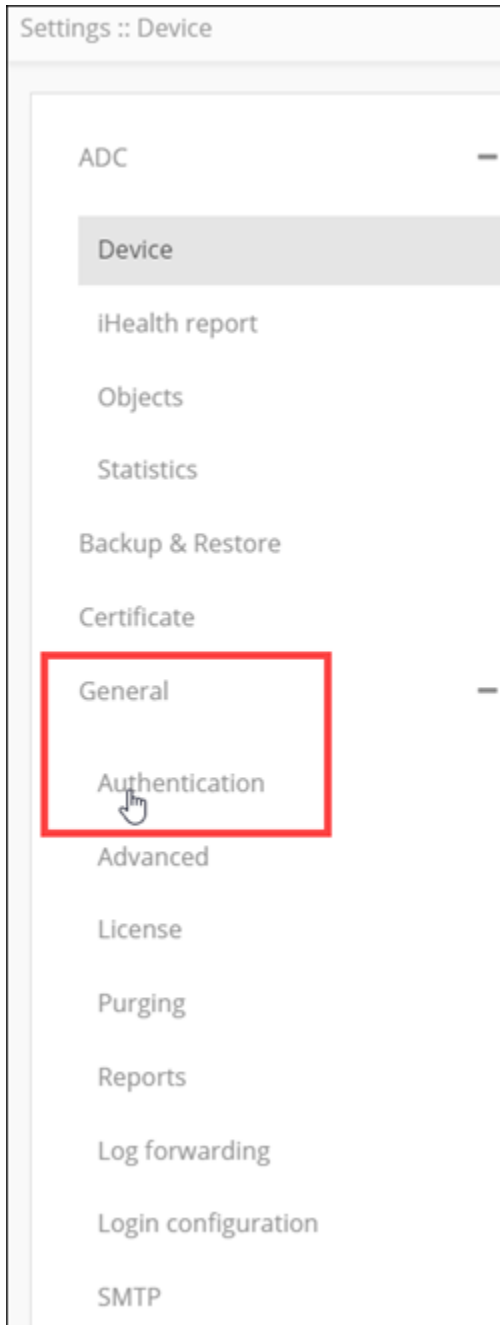
AppViewX integrates with RADIUS for authentication of external users.

To configure the RADIUS authentication:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

Settings :: Authentication

Quick config 0 Entries

ADC

LDAP TACACS RADIUS SSO IP Restriction Authentication settings OAuth Settings

General information

* Host

* Port 389

LDAPS ☒

Upload certificate Browse

Bind DN CN=admin,DC=example,DC=com

Bind password

Data center dc1

Authorization ☒

Enable Nested Groups ☒

LDAP Sync ☒

5. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click the **RADIUS** tab.

Settings :: Authentication

Quick config 0 Entries

ADC

LDAP TACACS RADIUS SAML IP Restriction Authentication settings

Server name Host Authentication mode Status

No records found

Save

*Server name

*Host

*Shared secret

*Authentication port

*Acceptance port

*Authentication mode ☒ RADIUS ☐ CHAP ☐ MS-CHAPv2 ☐ EAP-MD5

Authorization ☒

Authorization via ☒ Radius ☐ LDAP

*Vendor ID

6. Enter the following details (sample values are shown in the image below the table):

Field	Description
*Server name	Name of the RADIUS server.
*Host	The IP address of the RADIUS server.
*Shared secret	A unique key for authentication between the AppViewX server and the RADIUS server.
*Authentication port	Port number that AppViewX will use for authentication.

Field	Description
	 Note: The default authentication port number is 1812. Please check with your sysadmin if your organization uses a different port number.
*Acceptance port	Port number that AppViewX will use to accept a response from the RADIUS server.  Note: The default acceptance port number is 1813. Please check with your sysadmin if your organization uses a different port number.
*Authentication mode	Select one of the following authentication modes: • PAP/ASCII • CHAP • MS-CHAPv2 • EAP-MD5  Note: Ensure that the selected authentication mode is also confirmed in the RADIUS server settings.
*Authorization	In addition to authentication, AppViewX also lets you perform user authorization against the RADIUS server. To enable authorization along with authentication, turn on the toggle.  Note: If Authorization is not enabled, AppViewX will only carry out RADIUS authentication for the given user.
*Authorization via	Select from one of the following authorization modes: • RADIUS: To perform both, authentication and authorization, via the RADIUS server • LDAP: To perform authentication via the RADIUS server and authorization via the LDAP server

Field	Description
	 Note: This field is enabled only when the Authentication toggle is turned on.
*Vendor ID	Enter the vendor ID.  Note: AppViewX does not have a unique vendor ID. We use a free vendor ID: 500 . Ensure that this is configured as part of the RADIUS server settings.  Note: This field is enabled only when the Authentication toggle is turned on and authorization is done via the RADIUS server.
*Vendor type	Enter the vendor type.  Note: AppViewX does not have a unique vendor type. We use a free vendor ID: 200 . Ensure that this is configured as part of the RADIUS server settings.  Note: This field is enabled only when the Authentication toggle is turned on and authorization is done via the RADIUS server.
*LDAP	From the drop-down menu, select the LDAP server to be used for the authorization.  Note: This field is enabled only when the Authentication toggle is turned on and authorization is done via the LDAP server.
All * marked fields are mandatory.	

* Server name	radius
* Host	192.168.142.89
* Shared secret	
* Authentication port	1812
* Acceptance port	1813
* Authentication mode	☒ PAP/ASCII ☐ CHAP ☐ MS-CHAPv2 ☐ EAP-MD5
Authorization	☒
Authorization via	☒ Radius ☐ LDAP
* Vendor ID	500
* Vendor type	200



7. To save the RADIUS authentication settings entered above, click **Add** or to reconfigure the settings, click **Reset**.

The RADIUS authentication settings thus configured are saved and displayed in the table shown in the left half of the screen:

☐	Server name	Host	Authentication mode	Status	
☐	radius	192.168....	PAP	✓ Enabled	



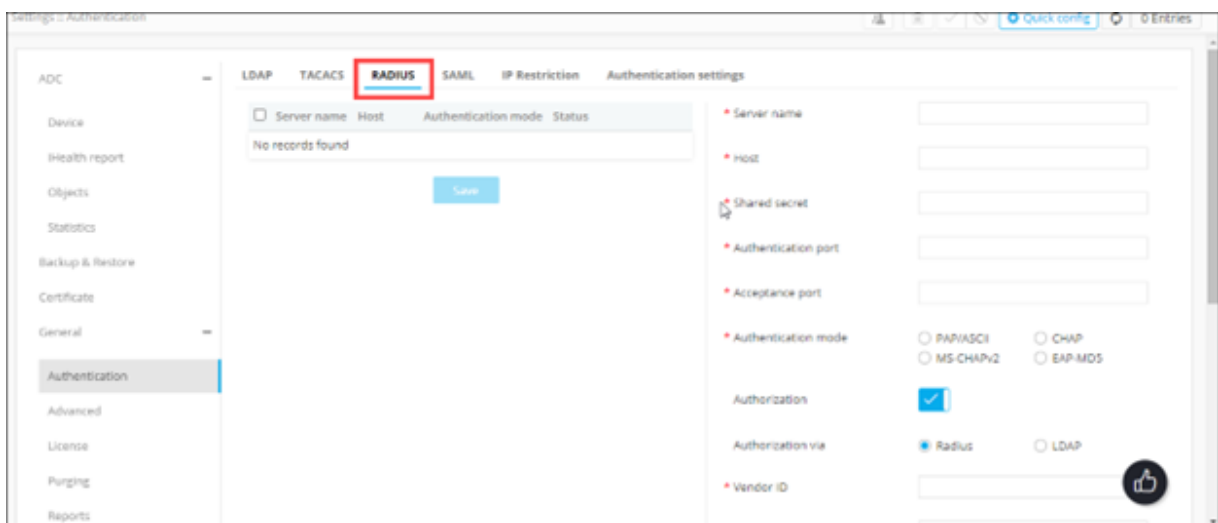
Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- Enabling a RADIUS Server for Authentication
- Disabling a RADIUS Server for Authentication
- Deleting a RADIUS Server

Enabling a RADIUS Server for Authentication

To enable a RADIUS server for authentication:

1. Navigate to the **Settings:: Authentication** page.
2. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click **RADIUS** tab.



3. From the table displayed in the left half of the page, for the server you want to enable, select the check box corresponding to the server name.

☒	Server name	Host	Authentication mode	Status
☒	radius	192.168.142.89	PAP	Disabled

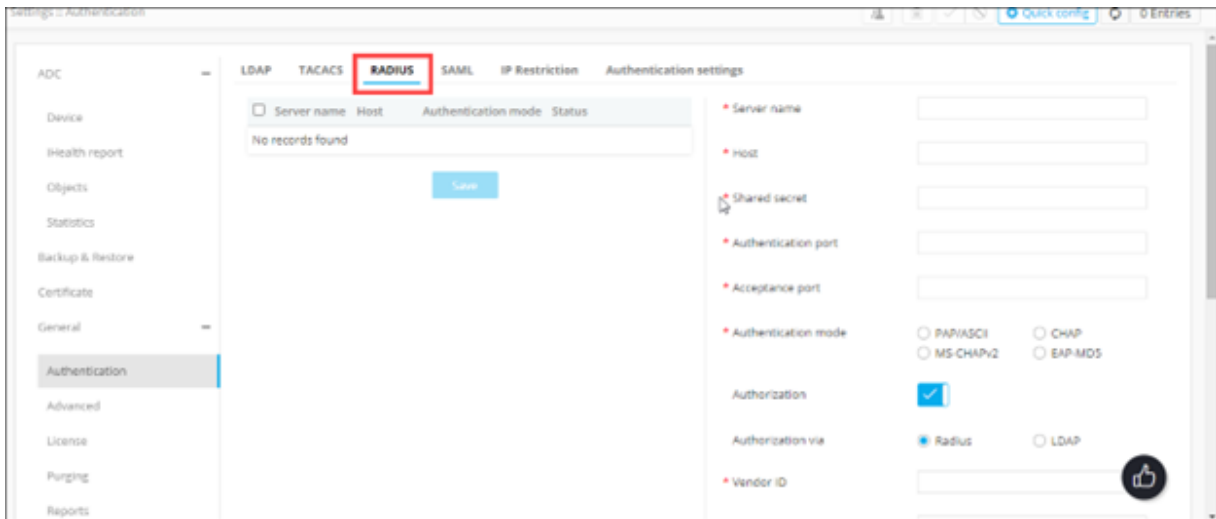


4. From the top-right corner of the page, click **Enable**.
5. In the **Confirmation** message dialog box, click **Proceed**.

Disabling a RADIUS Server for Authentication

To disable a RADIUS server for authentication:

1. Navigate to the **Settings:: Authentication** page.
2. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click the **RADIUS** tab.



3. From the table displayed in the left half of the page, for the server you want to disable, select the check box corresponding to the server name.

☒	Server name	Host	Authentication mode	Status
☒	radius	192.168.142.89	PAP	⊘ Disabled

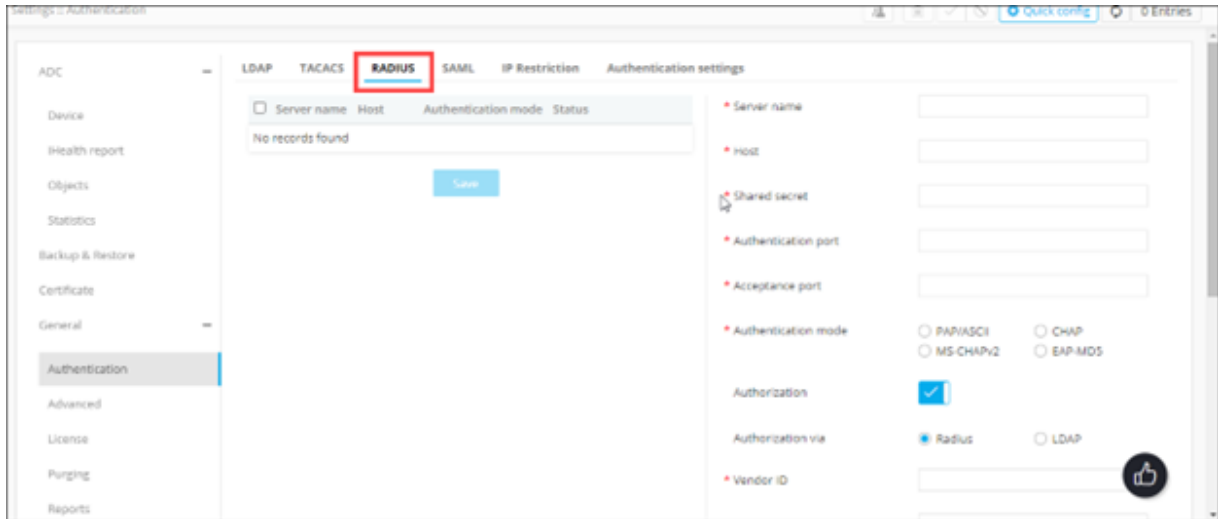


4. From the top-right corner of the page, click **Disable**.
5. In the **Confirmation** message dialog box, click **Proceed**.

Deleting a RADIUS Server

To delete a RADIUS server:

1. Navigate to the **Settings:: Authentication** page.
2. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click **RADIUS** tab.



- From the table displayed in the left half of the page, for the server you want to delete, select the check box corresponding to the server name.

☒	Server name	Host	Authentication mode	Status
☒	radius	192.168.142.89	PAP	⛔ Disabled



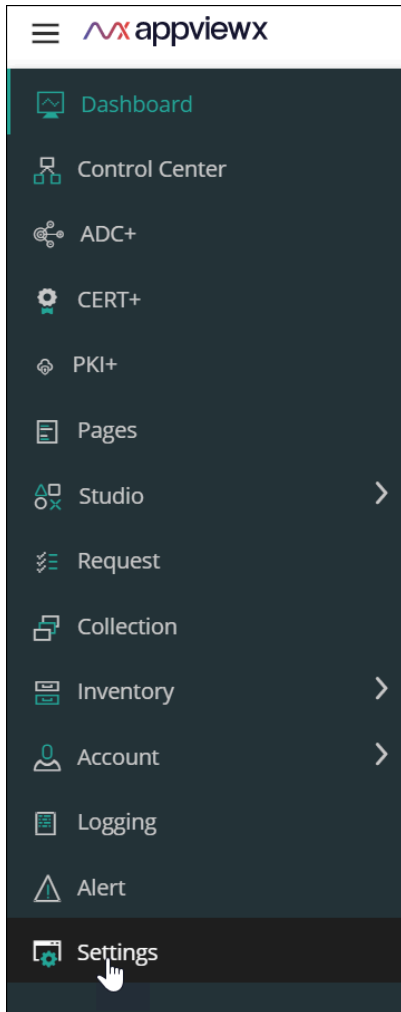
- From the top-right corner of the page, click .
- In the **Confirmation** message dialog box, click **Proceed**.

Configuring Single Sign On Settings with AppViewX

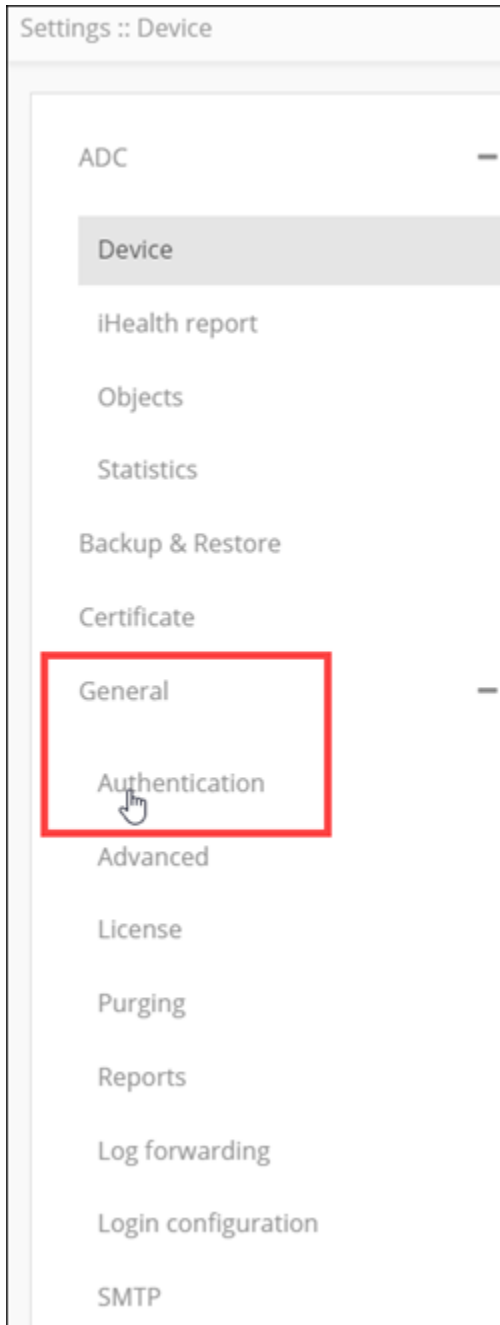
Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

To configure single sign on settings with AppViewX:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

Settings :: Authentication

Quick config 0 Entries

ADC

LDAP TACACS RADIUS SSO IP Restriction Authentication settings OAuth Settings

Device

iHealth report

Objects

Statistics

Backup & Restore

Certificate

General

Authentication

Advanced

License

Purging

Reports

Log forwarding

Login configuration

SMTP

General information

* Host

* Port 389

LDAPS ☒

Upload certificate

Bind DN CN=admin,DC=example,DC=com

Bind password

Data center dc1

Authorization ☒

Enable Nested Groups ☒

LDAP Sync ☒

- To configure the SSO settings, on the **Settings :: Authentication** page, click the **SSO** tab.

Settings :: Authentication

ADC

LDAP TACACS RADIUS SSO IP Restriction Authentication settings OAuth Settings

Device

iHealth report

Objects

Statistics

Backup & Restore

Certificate

General

Enable SSO ☐

The Enable SSO toggle is displayed (turned off by default).

- Turn on the **Enable SSO** toggle.

LDAP TACACS RADIUS SSO IP Restriction Authentication settings OAuth Settings

Enable SSO ☒

* Authentication Protocol ☒ SAML ☐ OIDC

The **Authentication protocol** field is displayed with the following options:

- **SAML**(selected by default)
- **OIDC**
- [Security Assertion Markup Language](#)
- [OpenID Connect- Overview](#)

Security Assertion Markup Language

- [SAML Overview](#)
- [Basic SAML Flow](#)
- [Configuration of SAML Parameters in AppViewX \(Service Provider\)](#)
- [Mapping User Groups for Local Authorization](#)
- [Troubleshooting](#)
- [Types of SAML Vendors](#)

SAML Overview

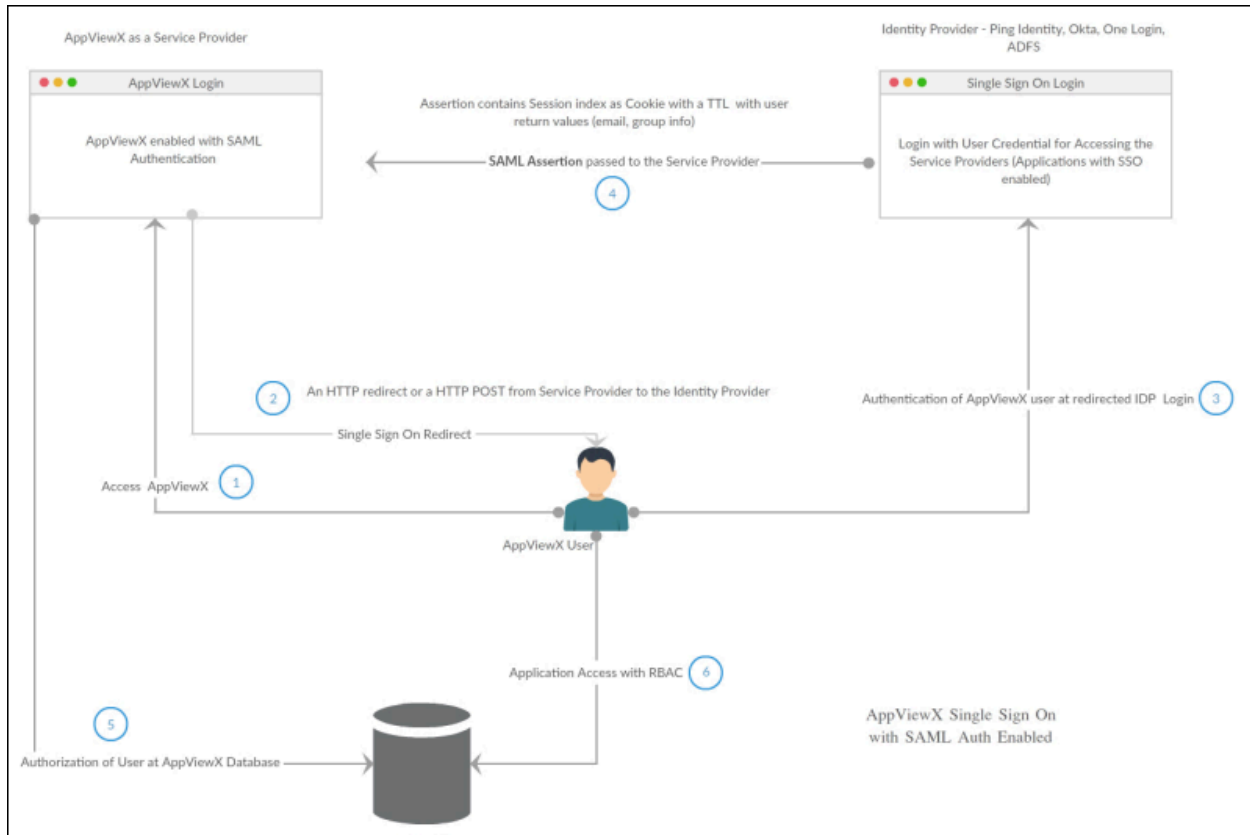
Security Assertion Markup Language (SAML) is a mechanism used for communicating identities between two web applications. It enables a web-based Single sign-on (SSO) and hence, it eliminates the need for maintaining credentials for various applications and reduces identity theft.

SAML integration requires the following parameters:

- IDP – Identity Provider (Okta, OneLogin, PingIdentity, and OpenSSO)
- SP – Service Provider (any application which supports SAML 2.0), AppViewX in this case
- User – Access the application

Basic SAML Flow

A user requests a SAML SSO to access a resource protected by a service provider. The service provider requests the identity provider to authenticate and authorize the user. The identity provider checks the existence of the user and sends back an assertion to the service provider that may or may not include the user information. The communication passes through the HTTP/HTTPS.



Configuration of SAML Parameters in AppViewX (Service Provider)

1. Under the **SSO** tab on the **Settings :: Authentication** page, enable the SSO toggle.
2. In the **Authentication Protocol** field, select the **SAML** option.
3. Enable the Enable SSO. This action will populate the service provider contents for the integration.
4. Under the **IDP Configuration** section, enter the required field information.

LDAP

TACACS

RADIUS

SAML

IP Restriction

Authentication settings

Enable SSO ☒

IDP Configuration

Meta data

Browse

* Issuer URL

* SSO URL

SLO ☒

* SLO URL

* Upload certificate

Browse

Default login :

To access default login page when SAML is enabled : <https://aab4320.my.idaptive.app/appview/login> (or) <https://aab4320.my.idaptive.app/appview/login> (in the case of load balanced web configuration).

Assertion parameters :

Following values are expected in the SAML assertion from the IDP in the mentioned format

Attributes	Claims Values to be mapped in IDP
FirstName	map to users firstname in IDP
LastName	map to users lastname in IDP
EmailId	map to users email in IDP
Mobile	allowed to pass an empty value
NameID	map to users email or login email in IDP
Roles	map to security or user groups in IDP

Note :

Use local authorization if roles are not passed in assertion

The following table describes the field information in this section:

Field	Description
Meta data	Upload the Metadata which is downloaded from your Identity Provider.  Note: Upload of metadata automatically parses the fields SSO, SLO, and so on.
*Issuer URL	 Note: This field is auto-populated upon uploading of the Meta data. In case the Meta data is unavailable, enter the ID of the Identity Provider.
*SSO URL	 Note: This field is auto-populated upon uploading of the Meta data. In case the Meta data is unavailable, enter the SSO URL which is a single sign-on URL for the service provider to authenticate the users.
SLO	Enable/Disable SLO as per requirement.
*SLO URL	 Note: This field is auto-populated upon uploading of the Meta data. In case the Meta data is unavailable, enter the SLO URL which is the SAML logout URL to send logout responses.

Copyright © 2023 [AppViewX, Inc]. All Rights Reserved.

42

Field	Description
*Upload certificate	Upload the IdP certificate in .pem format if it is not available as a part of your IdP metadata.
All * marked fields are mandatory.	

5. Under the **Service Provider Information** section, enter the required field information.

Service Provider Information

Host

https://int-betapartner.appviewx.plus

Entity ID

https://int-betapartner.appviewx.plus/appviewx

Service URL

https://int-betapartner.appviewx.plus/appviewx/ssoLogin

SLO URL

https://int-betapartner.appviewx.plus/appviewx/logout

Sign AuthN Request.

☐

SP metadata

Download

The following table describes the field information in this section:

Field	Description
Host	Enter the host information for AppViewX in the Hostfield. The host information can be the Hostname/URL used to access the application.  Note: The Entity ID, SSO URL and the SLO URL fields will be auto-populated based on the Host information provided.
Entity ID	 Note: This field is auto-populated based on the Host information provided.

Field	Description
Service URL	 Note: This field is auto-populated based on the Host information provided.
SLO URL	 Note: This field is auto-populated based on the Host information provided.
Sign AuthN Request	Enable/Disable the Sign AuthN Request toggle to send signed AuthN requests from AppViewX to your Identity Provider.  Note: This is to be enabled only when your IdP requires a sign authN request from service provider. Once the Sign AuthN Request is enabled, Upload a Service Provider certificate and private key in a p12 format and provide the p12 Password. Choose the Signing Algorithm (Recommended Algorithm: SHA-256) from the drop-down list. The Service provider certificate should be shared with the IDP to validate the Service Provider SAML assertion signature.
SP metadata	Download the Service Provider information (Entity Id, SSO/Service URL, SLO URL) to be consumed at IdP.

6. Under the **Advanced** section, enter the required field information.

Advanced

Local authorization ☐

Name Id Format

Email Address

Authn Context

urn:oasis:names:tc:SA... X

Auth Comparison

Exact

Save

Cancel

Reset

The following table describes the field information in this section:

Field	Description
Local authorization	Enable/Disable the Local authorization to authenticate in IdP and authorize in AppViewX. If the IDP is unable to pass the roles/usergroup as a part of the SAML assertion and requires AppViewX to perform the Authorization then the above feature can be used.  Note: This feature is available from 20.1 version of AppViewX.
Name Id Format	Choose the Name id Format from the drop-down list.
Authn Context	Enter the Authn Context in the text field. Use any one of the below values for a customized type of authnrequest needed by your IDP. Other RFC SAML2.0 standard authnrequest can also be used. (Copy and paste the below values or add values in the same format from RFC to the AuthNcontext field). • urn:oasis:names:tc:SAML:2.0:ac:classes:X509. • urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient. • urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport • urn:oasis:names:tc:SAML:2.0:ac:classes>Password • urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos • urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

Field	Description
Auth Comparison	Choose the Auth Comparison from the drop-down field. This indicates how the authentication context URI in the AuthnRequest message compares to the context defined at the asserting party. It is preferred to be exact.

7. Click **Save**.
8. If the configuration provided needs to be removed, click **Reset**.

Mapping User Groups for Local Authorization

Administrators can map user groups manually for external users login through SSO by using either Manual mapping or Birthright.

Manual Mapping

Once the user logs in to AppViewX using SSO if no proper Roles are passed in the Assertion the user will end on a No Usergroup found page. Now the administrator can log in with the default login URL **https://ip:port/appviewx/login** and navigate to Account > Users. The user who has not logged in will have the user-created tag and will be in an inactive state. Administrators can modify the user and map the user to a user group that is available and this will enable the user to login successfully on the next attempt.

Birthright Role

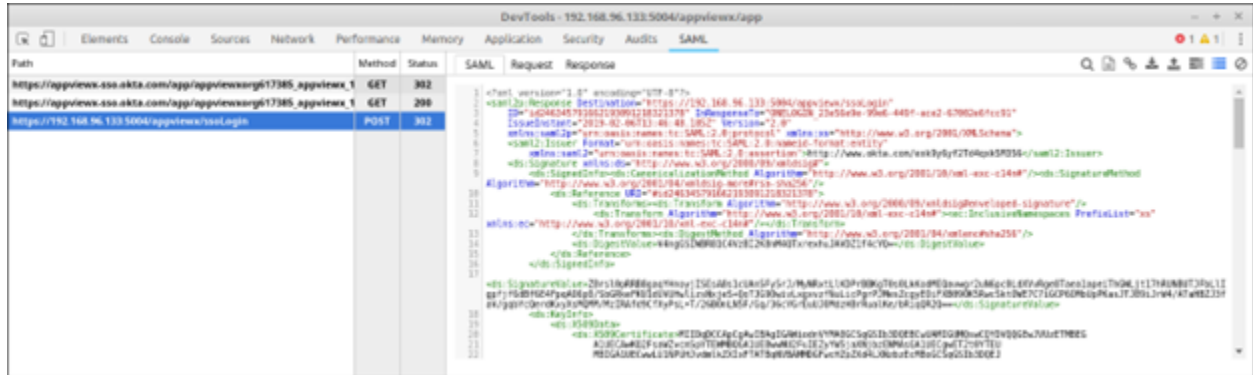
The administrator can enable a birthright role and map a user group by default for all the sso users to log in initially when they do not have a role/user group passed in the SAML assertion. This would enable the user to login successfully and access the application with the access given in the specific user group. If required now the administrator can create different sets of user groups and assign manually to the respective users who do not need the birthright user group which will be reflected in the subsequent login.

Troubleshooting

Enable the SAML extension in the browser. While performing the login, enable the DEV tools and open the SAML tab. During the operation, the SAML assertions are passed in the HTTP headers. Similar to the external authentication configuration, if the role name passed in the SAML assertion matches the role name in the AppViewX database, the login will be successful.

Sample Configuration of SAML Assertion

Number of SAML Assertions in HTTP Headers



Sample SAML Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response Destination="https://192.168.x.x:31443/appviewx/ssoLogin"
ID="id246345791662193091218321378" InResponseTo="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
IssueInstant="2019-02-06T13:46:48.185Z" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk9y6yf2Td4qxk5M356</saml2:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#id246345791662193091218321378">
<ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="xs"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
</ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256"/>
<ds:DigestValue>V4ngSIWBR81C4VzBI2K8nM4QTxreXhuJAVDZ1f4cYQ=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>ZBrs10pRRB8gaqYHnoyJlSEsA8s1cUAn5Fy5rJ/MyNrXtLIKPrBBKGT0sOLkKodMEQavwgr2uN6pc0LDxVvRge8Taea1apeiThGWLjt17hRU
NBUTJfBlIlgpfj6dBf6E4FpqAO6p0/SbGRkeFKU1dUVUHWlzsNxjeS+QoTJG9OwivLxgxvzfNuLicPgrPJMesZcgyEOiFXB09OK5RwcSkOWE7C7iGCP6OMbUpP
KasJTJ89iJrW4/ATaHBZJ3faV/gqbYcQerdKxyXsMQMM/MzIRaFd9CfXyP5L+T/26BOnLN5F/Gq/36cYGrEuUJ0MdZHBrrualKe/bRiqQR2Q==</ds:SignatureVal
ue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDqDCCApCgAwIBAgIwVMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVZETMBEg
```

```

A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFtATBgNVBAMMDGFwcHdpZD4LNzZEcMBBoGCSqGSib3DQJEJ
ARYNaW5mb0Bva3RhLmNvbTAeFw0xOTAyMDEwOTQ4MjJaFw0yOTAyMDEwOTQ5MjJaMIGUMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFtATBgNVBAMMDGFwcHdpZD4LNzZEc
MBoGCSqGSib3DQJEJARYNaW5mb0Bva3RhLmNvbTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAIc22r1CR7gbMVcyYnRjkDLGRwHJ1zhQkWTVoEZdbk/KTHwVMXHpNinkOhUcxbzfHePBf6wx
9jETHiNvvHZVlg6ZktYotG9DF/FF0fM:zhzfwqR5yt27ihuiVTeGT8GjNcXwOoyzJdrDuZg27ybl
jriqGPKrLiwrrot54R1LP2VclM0FdIOWdOoU1N5IEEnFAd+2UECZZLQ0gJrDpFcbDisuhmp5bTKUS
1RplxarNeacH2kIRY4efeqQdVgaghs+zMN44iz+YGs8uELEIKerOabEtoYITJmsVnqEcs8fUvKx
LLdZevPhh89v0MJiZi9gTjttf9N+NEUzyJsHfxqmnUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
RZo42x1gDE3d9nftXr2LoUltdTQeVoFdkiJlqJla21kDRcWHis2OvuFwOW+QdUeh5uUljGxbhaA
cQleJUvuD1aEK/ynUDKGA0jvdLR7IbwTK69i7c19F7pti6b5sq8yl5fOavit1N3INlzZdkrPIP1
hJnKcjOSVyMPv8a7rDXOtXxDoZgi+pWj0qlp4E9tKOrWJgKdjS8j03uIWwtOx4Jak4yYueaY8nH1
+amyE6w96Qm6ScEGLcxXzbocS7BMjZOM4Mr6zXOTS8pU+AX6NBmdNkdwO9JSeXm3U6IRWv59jet
qMeKqf4aKRg+oqbw9hkH3X6qT69AeEiPz6YPmQ==</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</ds:Signature>

<saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status>

<saml2:Assertion ID="id24634579166299789832980116" IssueInstant="2019-02-06T13:46:48.185Z"

Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:xs="http://www.w3.org/2001/XMLSchema">

<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"

xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk9y6yf2Td4qk5M356</saml2:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI="#id24634579166299789832980116">

<ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="xs"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>

</ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>

<ds:DigestValue>hnTKZKSyxKC6WGZTK7iD+iQv4+nj/91eX8vhrkyi+1k=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

```

```

<ds:SignatureValue>OtgpfXWkII00hSZiHpAdTDBg6v11+/unBzyPOFSBI+0+b2i22s3IHtzCqsEVp4Xn9J1XoL12tCr/uhg7b4kxcTslMsAYFVQipUZLkanElaEOSv2
tnjQuAoE3fBMtm2d/3+nlXofyGiOMEY5OrFaGGjC9ZAMk2qJDAEzjZHhjOyoolQltzDocIVFvXeFSI/bAaDNSRPYT0B9dXsGpjpUIA6CMpmJXSxgAPwogaM20d48
o7iKi3THjTgm1L2z9nntQajfaRERkoTfAV0sGE6iKIUahWmtMkUDOUXbMeBXo61cpQ5A/WsfxbpZKhJkDes/9lzcDoPkl7w+TshJnQMQA3A==</ds:SignatureVal
ue>

  <ds:KeyInfo>

    <ds:X509Data>

      <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAWiodnVYMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
        A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
        MBIGA1UECwwLU1NPUHJvdmlkZXlxFtATBgNVBAMMDGFwcHZpZXd4LXNzbzEcMBoGCSqGSIb3DQEJ
        ARYNawW5mb0Bva3RhLmNvbTAeFw0xOTAyMDEwOTQ4MjJaFw0yOTAyMDEwOTQ5MjJaMIGUMQswCQYD
        VQqGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
        A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXlxFtATBgNVBAMMDGFwcHZpZXd4LXNzbzEc
        MBoGCSqGSIb3DQEJARYNawW5mb0Bva3RhLmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
        ggEBAIc22r1CR7gbMVcyYnRjkDLGRwHJ1zhQkWTVoEZdbk/KTHwVMXHpninkOhUcxbzfHePBf6wx
        9jEThiNvHZVlg6ZktYotG9DF/FF0fMxhzfweqR5yt27ihiuVTeGT8GjNcXwOoyzJdrDuZg27ybl
        jriqGPKrLiwrrot54R1LP2VclM0FdIOWdOoU1N5IEFAd+2UECZZLQ0gJrDpFcbDisuhmp5bTKUS
        1RplxarNeach2kIRY4efeqQdVgaghgs+zMN44iz+YGs8uELEIKerOabEtoYiTJmsVnqEcs8fUvKx
        LLdZevPhh89v0MjZl9gTjtf9N+NEUzyJsHfxqmnUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
        RZo42X1gDE3d9xnftXr2LoUItDQeVoFdklJlqJla21kDRCwHis2OvuFwOW+QdUeh5uUljGxbhaA
        cQleJUvuD1aEK/jynUDKGA0jvdLR7lbwTK69i7c19F7pti6b5sq8yjl5fOavit1N3INlzZdkrPIP1
        hJnKcjOSVvMPv8a7rDXOtXxDoZgi+pWj0qlp4E9tKorWJgKdjS8j03ulWwtOx4Jak4yYueaY8nH1
        +amyE6w96Qm6ScEGLcxZboczS7BMjZ0M4Mr6zXOTS8pU+AX6NBmdNkdwo9JSeXm3U6lRWv59jet
        qMeKqf4aKRg+oqbw9hkH3X6qT69AeEiPz6YPmQ==</ds:X509Certificate>

    </ds:X509Data>

  </ds:KeyInfo>

</ds:Signature>

<saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

  <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">saml@appviewx.com</saml2:NameID>

  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml2:SubjectConfirmationData
InResponseTo="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"

    NotOnOrAfter="2019-02-06T13:51:48.185Z" Recipient="https://192.168.x.x:31443/appviewx/ssoLogin"/></saml2:SubjectConfirmation>

</saml2:Subject>

<saml2:Conditions NotBefore="2019-02-06T13:41:48.185Z" NotOnOrAfter="2019-02-06T13:51:48.185Z"

  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

  <saml2:AudienceRestriction>

    <saml2:Audience>https://192.168.x.x:31443/appviewx/</saml2:Audience>

```

```

</saml2:AudienceRestriction>

</saml2:Conditions>

<saml2:AuthnStatement AuthnInstant="2019-02-06T13:46:46.836Z"
  SessionIndex="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

  <saml2:AuthnContext>

    <saml2:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>

  </saml2:AuthnContext>

</saml2:AuthnStatement>

<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

  <saml2:Attribute Name="EmailId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml@appviewx.com</saml2:AttributeValue>

  </saml2:Attribute>

  <saml2:Attribute Name="FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml</saml2:AttributeValue>

  </saml2:Attribute>

  <saml2:Attribute Name="LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">appviewx</saml2:AttributeValue>

  </saml2:Attribute>

  <saml2:Attribute Name="NameID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml@appviewx.com</saml2:AttributeValue>

  </saml2:Attribute>

  <saml2:Attribute Name="Mobile" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">0</saml2:AttributeValue>

  </saml2:Attribute>

  <saml2:Attribute Name="Roles" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">oktarole</saml2:AttributeValue>

  </saml2:Attribute>

</saml2:AttributeStatement>

</saml2:Assertion>

</saml2p:Response>

```

The data in bold contains the attributes passed to AppViewX for a successful login. If this data is not passed in assertion, the assertion must be revisited.

Vendors Certified with AppViewX

AppViewX has been certified with the below SAML 2.0 enabled SSO vendors:

- Okta
- OneLogin
- ADFS
- Forgerock
- Idaptive
- Azure
- ADFS
- PingIdentity

Types of SAML Vendors

Types of SAML Vendors

- Okta
- OneLogin
- ADFS
- Forgerock
- Idaptive
- [ADFS Integration](#)
- [Okta Integration](#)
- [Forgerock Integration](#)
- [OneLogin Integration](#)
- [Idaptive Integration](#)

ADFS Integration

The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

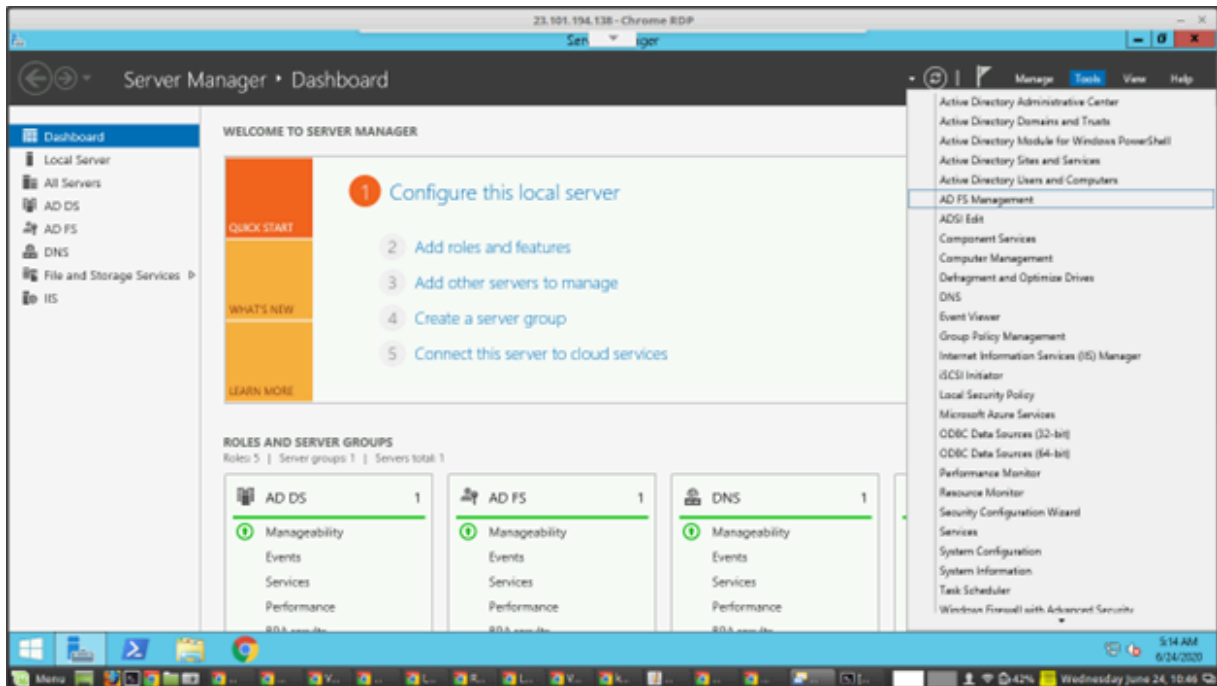
Prerequisite

To enable ADFS based single sign-on, the ADFS service should be installed and configured with the respective Active Directory Domain.

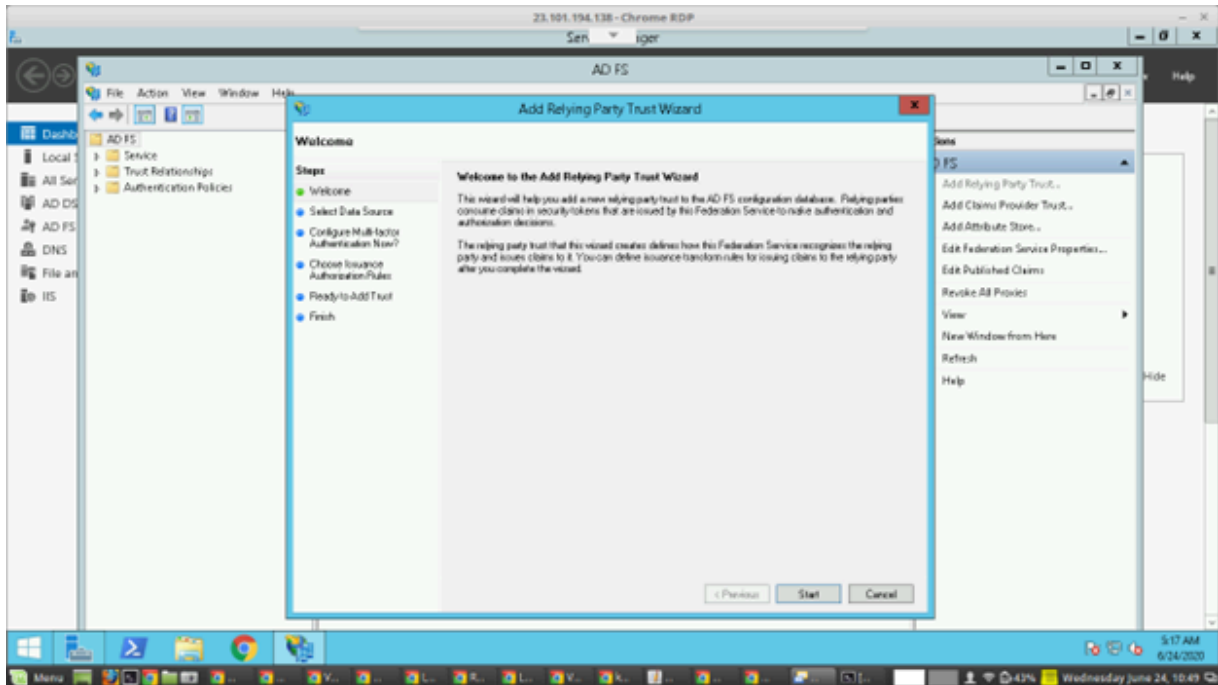


Note: The steps are performed on the Windows 2012 R2 server with AD enabled in the same domain.

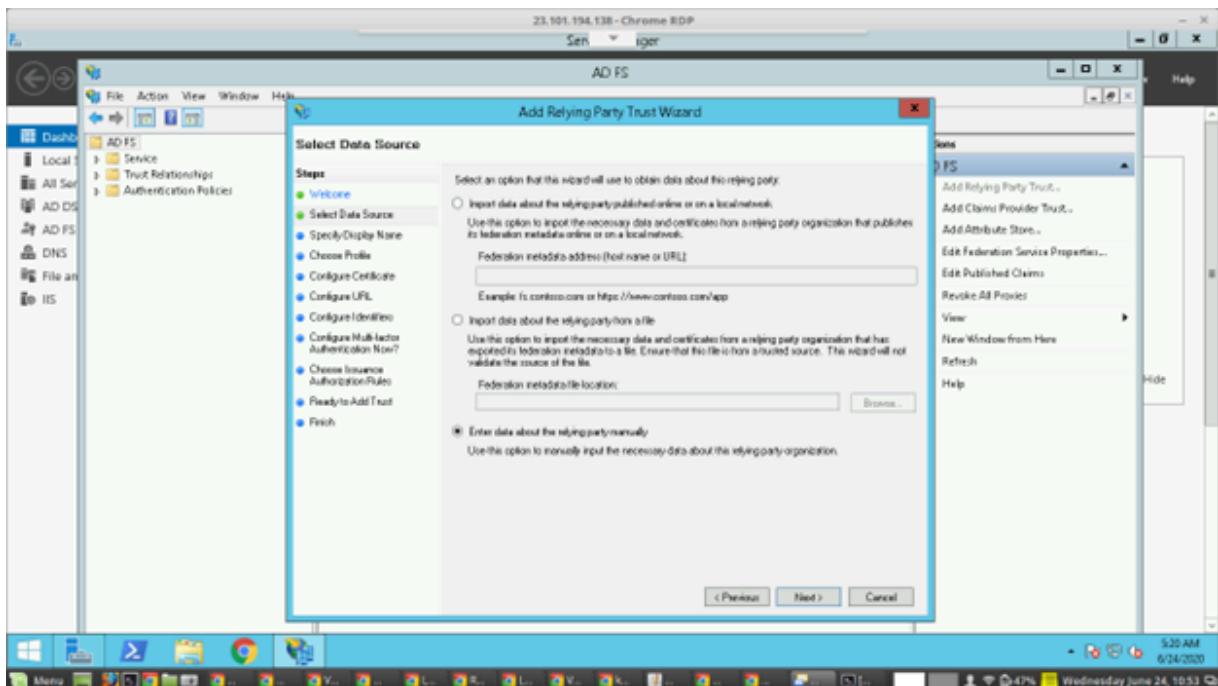
1. Navigate to **Server Manager > Tools > AD FS Management**.



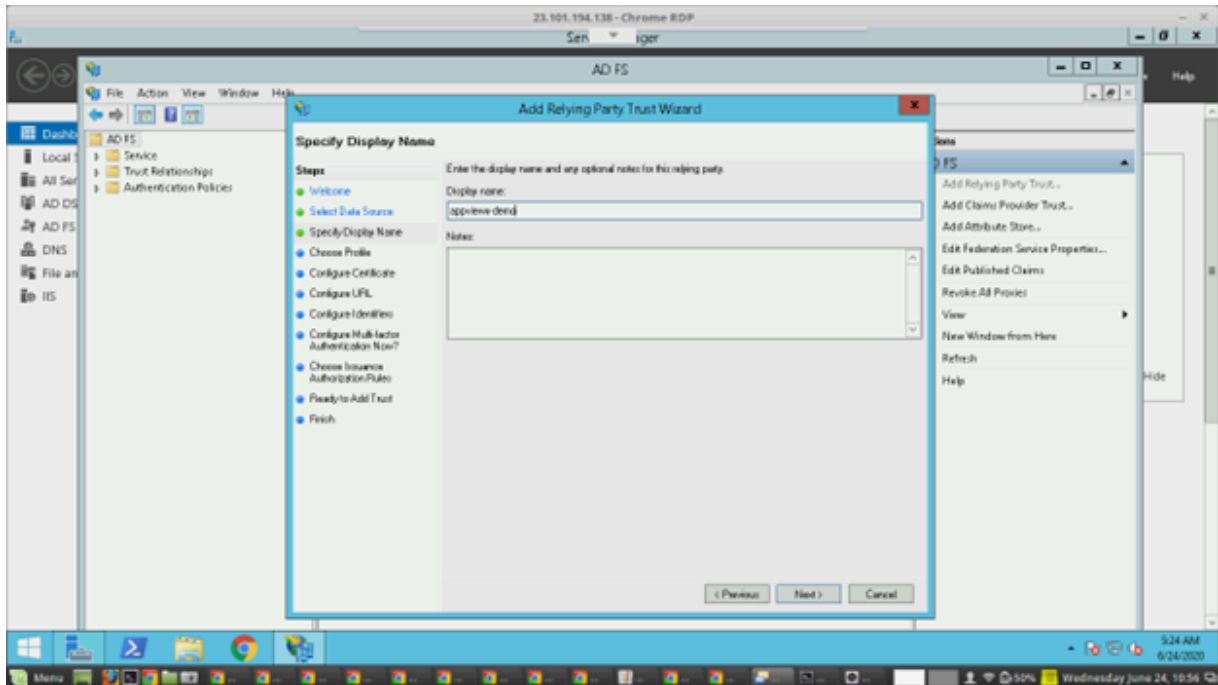
2. In the **AD FS** window, under **Actions** select **Add Relying Party Trust**.



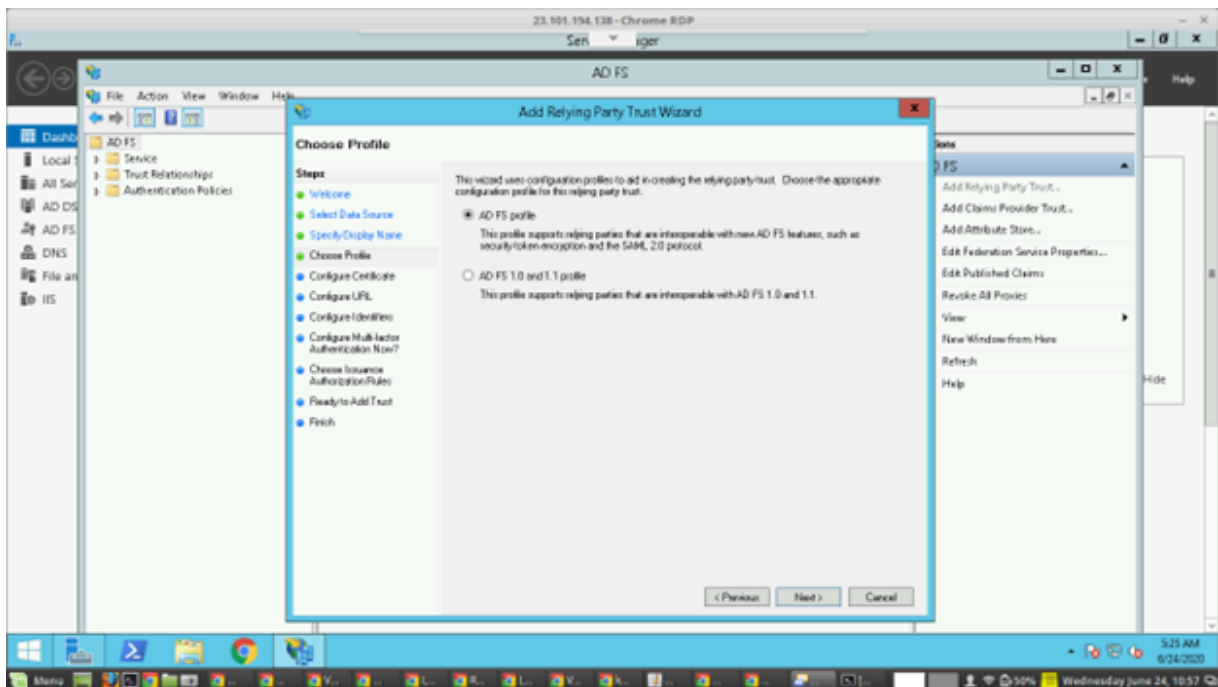
3. Start the **Add Relying Party Trust wizard**.
4. Under the **Select Data Source** section, select the **Enter data about the relying party manually** option and click **Next**.



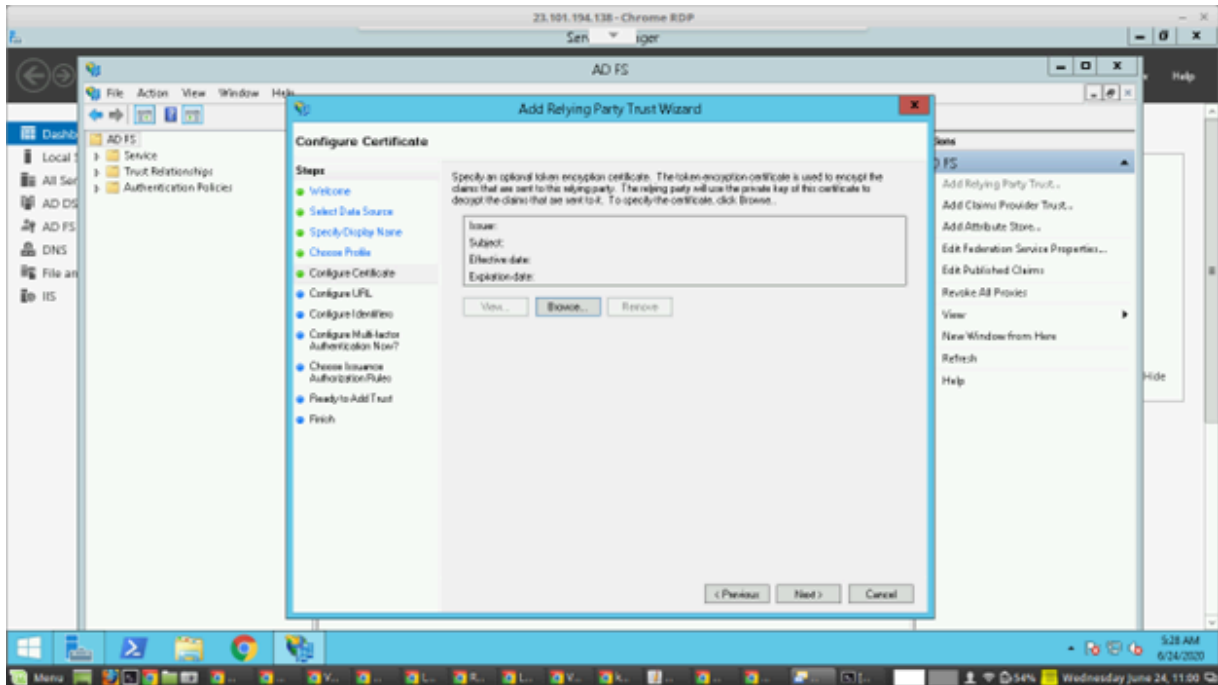
5. Enter a **Display Name** and click **Next**.



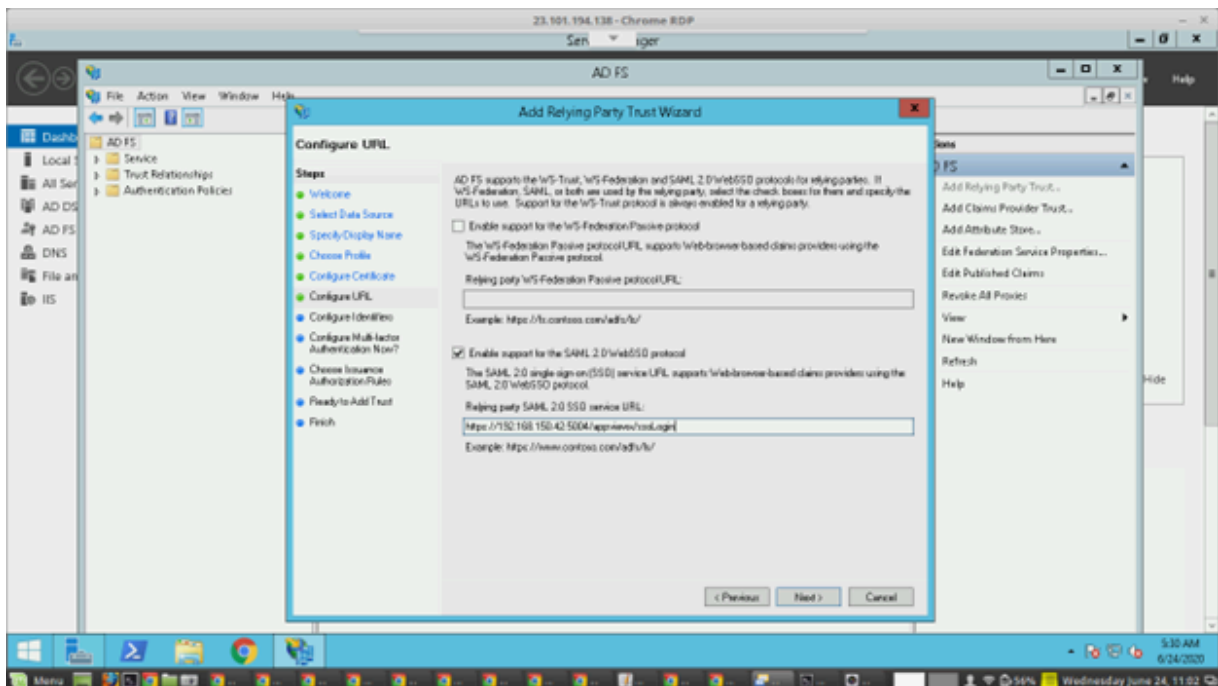
6. Under the **Choose Profile** section, select the **AD FS profile** option and click **Next**.



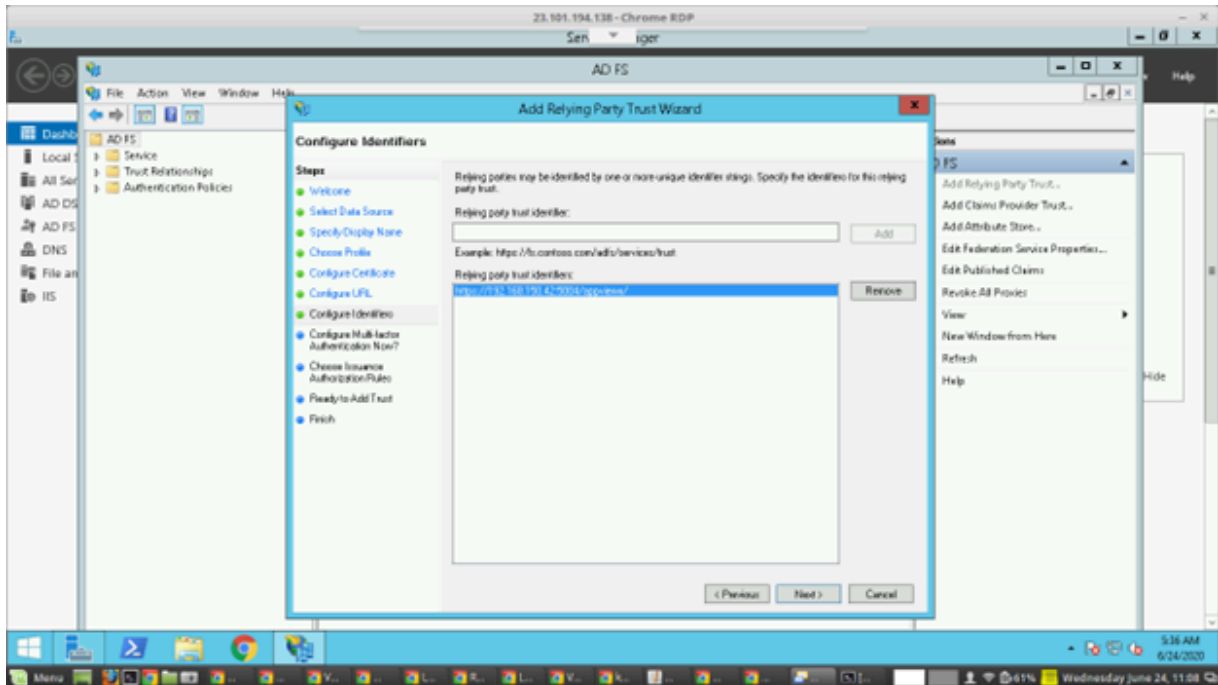
7. Add a new token encryption certificate if needed or leave it with the default setting and click **Next**.



8. Under the **Configure URL** section, select the **Enable support for SAML 2.0 WebSSO protocol** option and enter the AppViewX Service URL which was copied in the previous step of Enabling SSO in AppViewX and click **Next**.

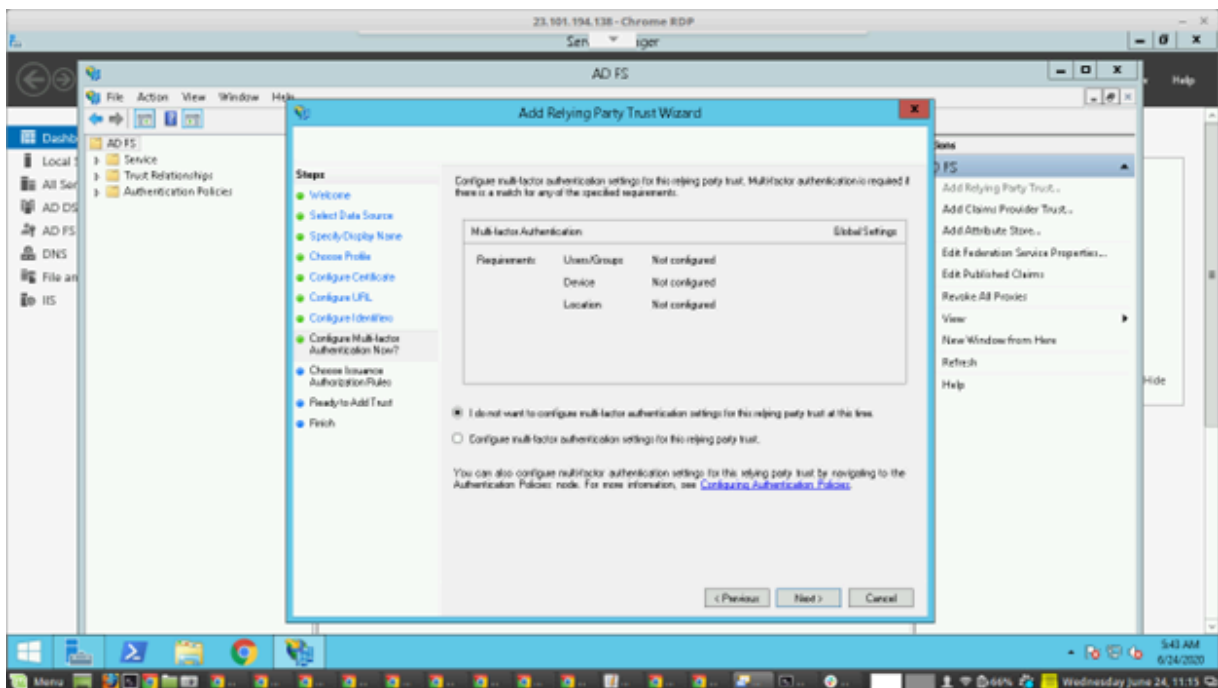


9. Under the **Configure Identifiers** section, enter the **AppViewX Entity ID** which was copied in the previous step of Enabling SSO in AppViewX and click **Add**.

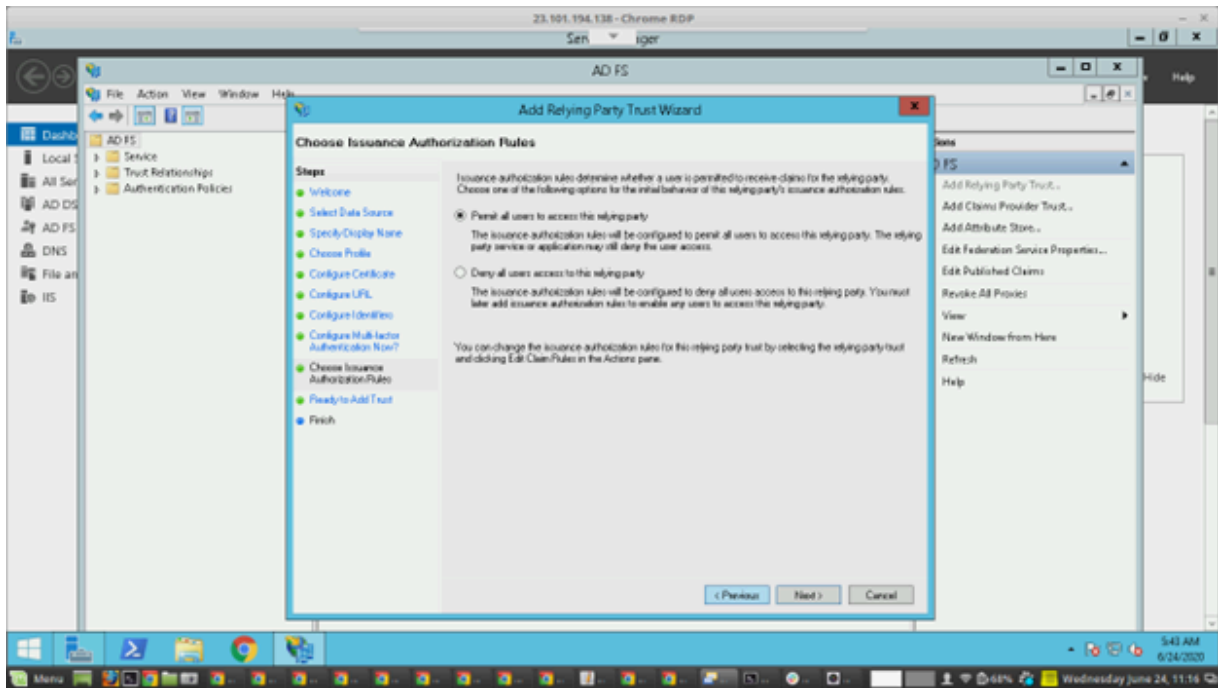


10. Click **Next**.

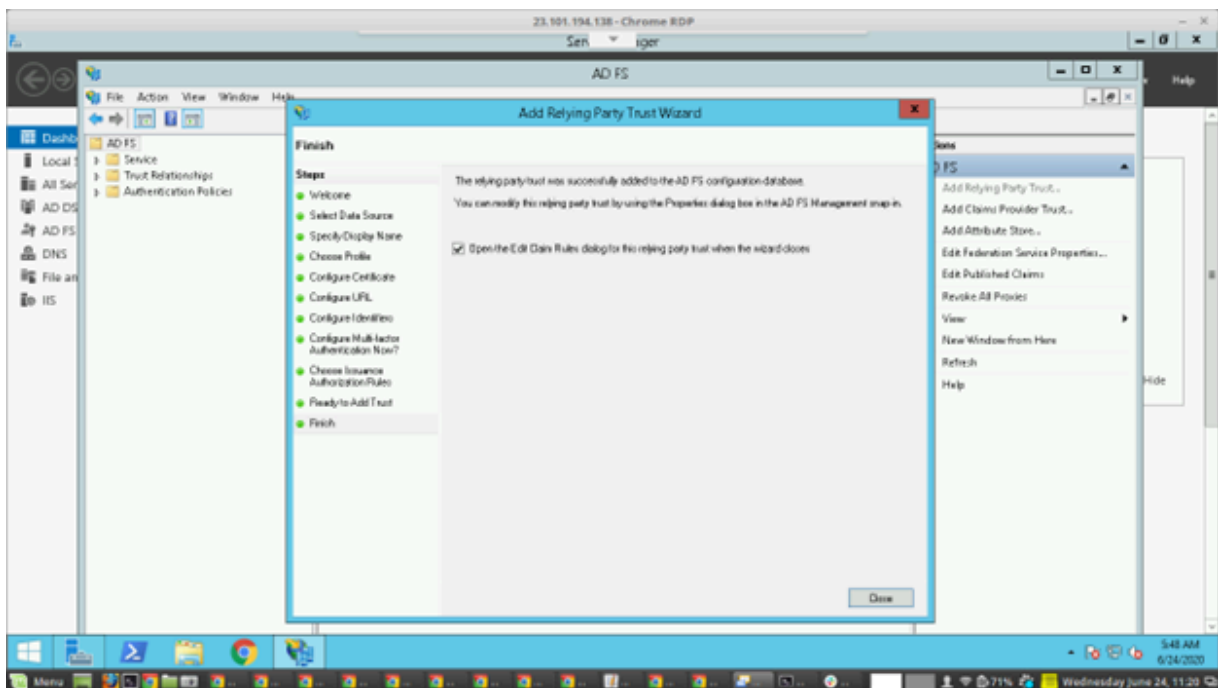
11. Under the **Choose Multi-factor Authentication** section, select the **I do not want to configure multi-factor authentication settings at this time** option. If the organization has a multi-factor authentication setting, enable it and click **Next**.



12. Under the **Choose Issuance Authorization Rules** section, select **Permit All Users to access this relying party** and click **Next**.



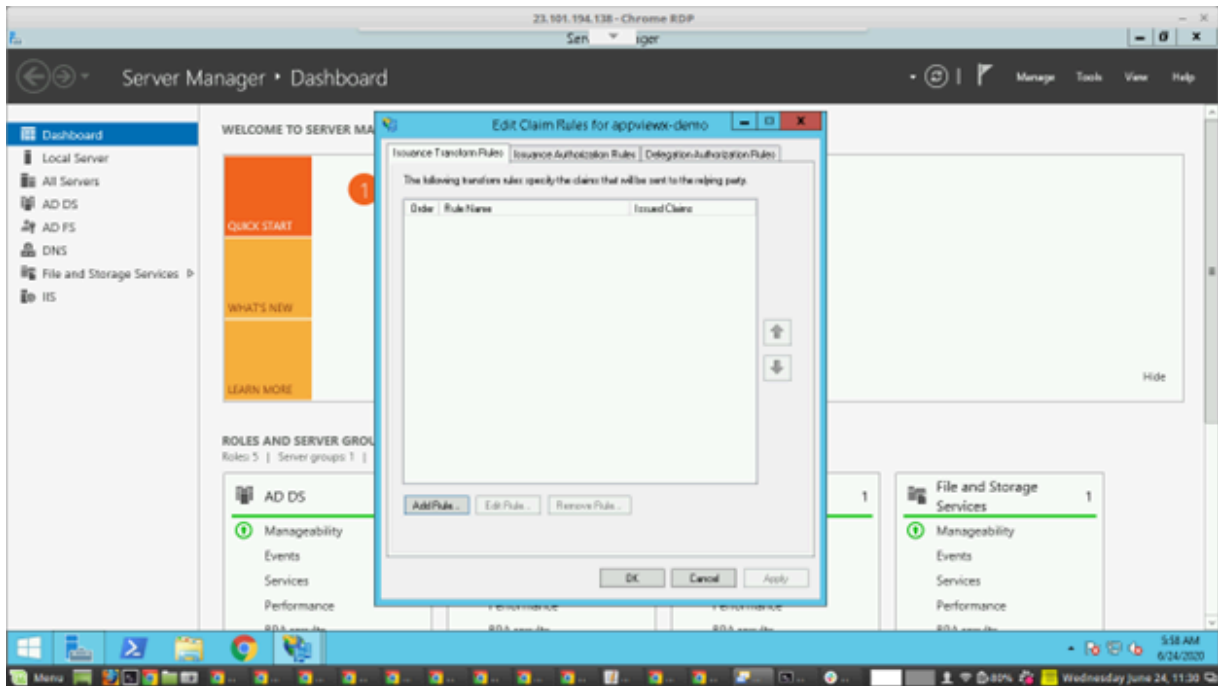
13. Under the **Ready to Add Trust** section, review the configuration done in the wizard and click **Next**.
14. Under the **Finish** section, select the **Open the Edit Claims Rules dialog for this relying party trust when the wizard closes** checkbox and click **Close**.



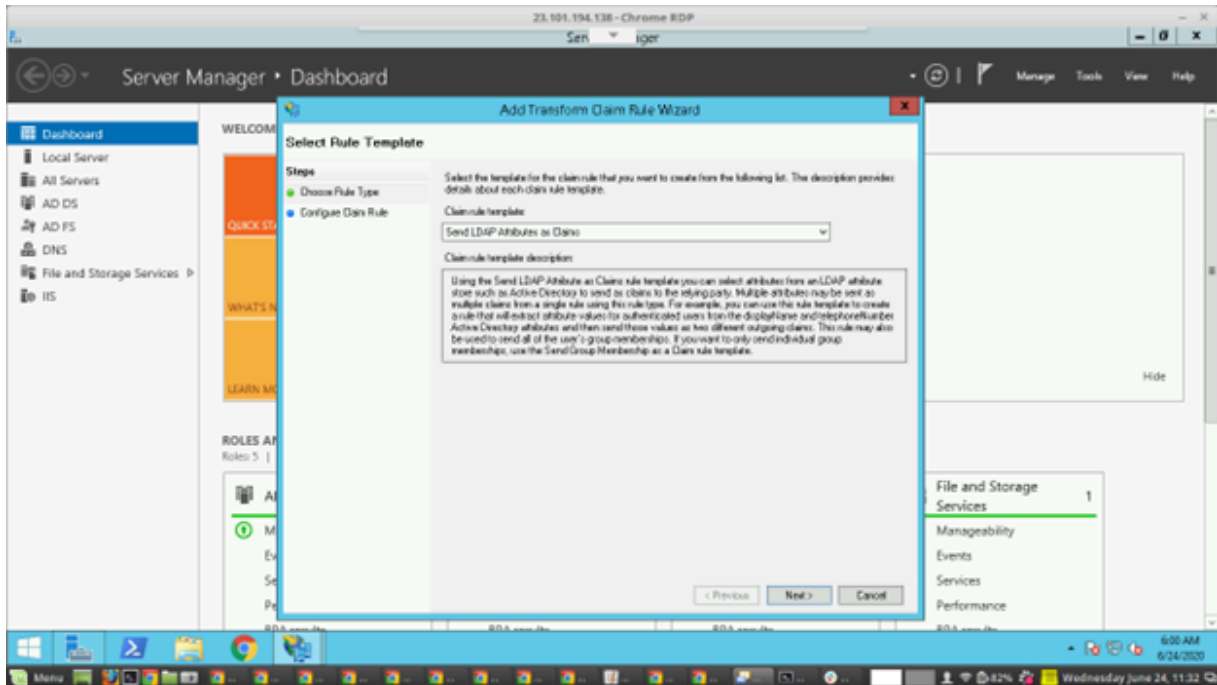
Add Claim Rules

To configure attributes or claims to be passed as an assertion Claim Rules should be created in ADFS.

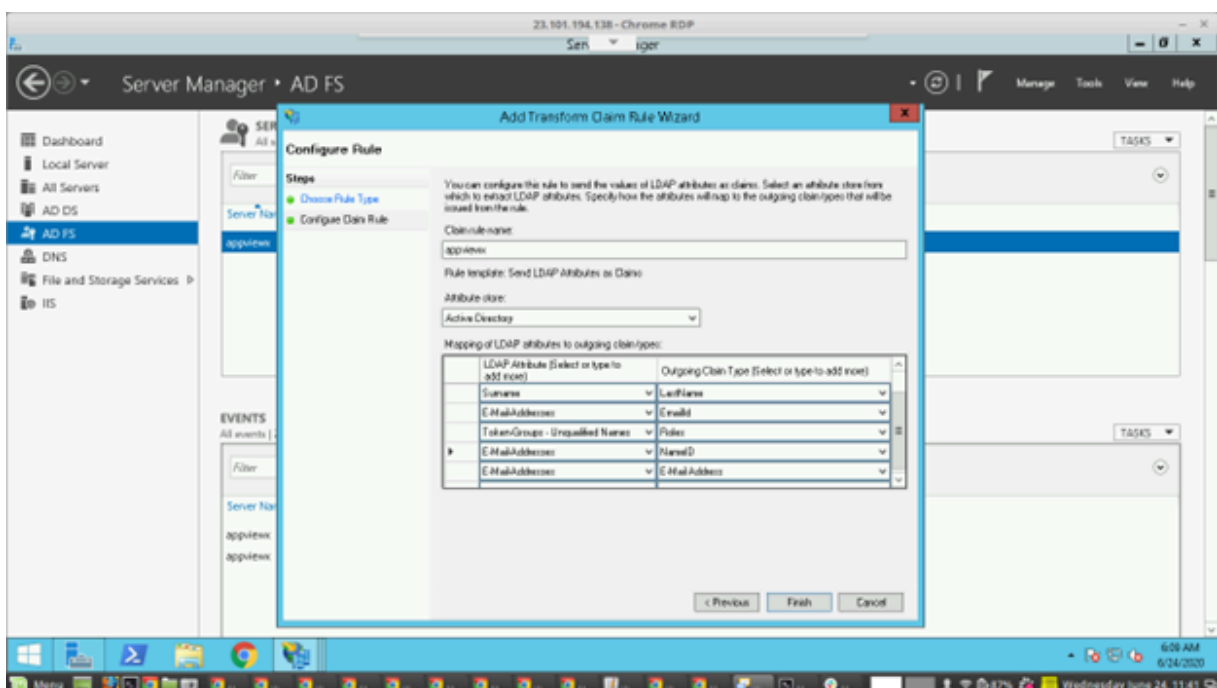
1. In the **Edit Claim Rules** pane click **Add Rule**.



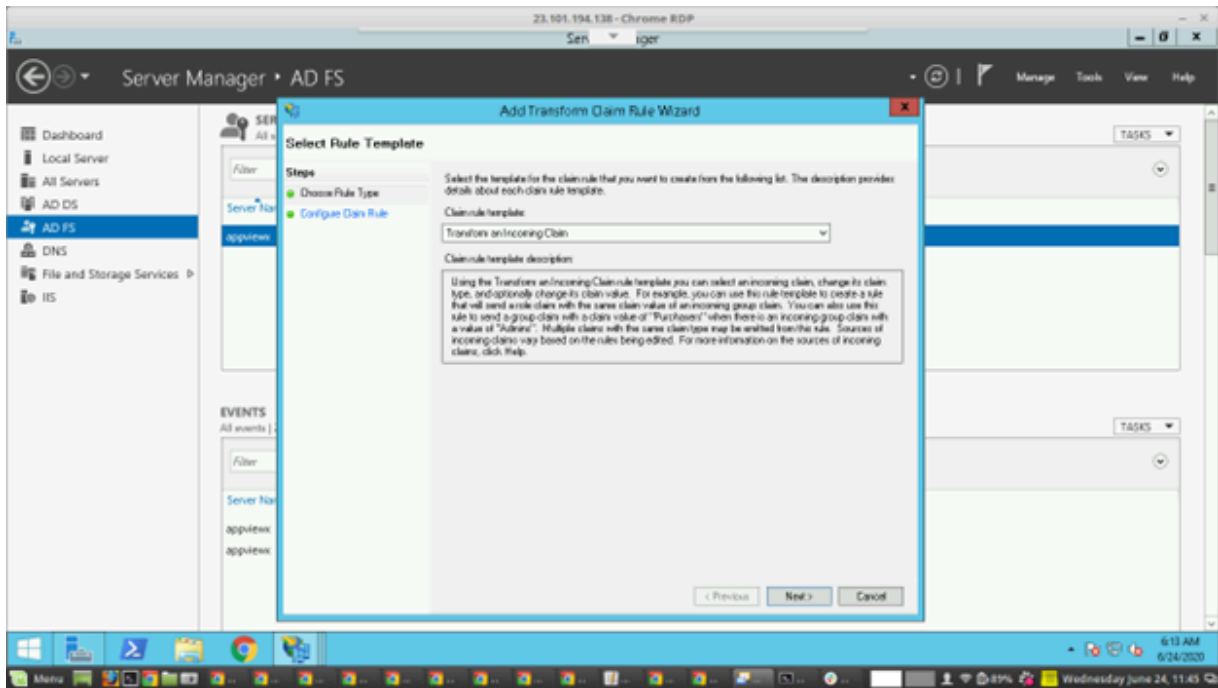
2. Under the **Select Rule Template** section, select **Rule Type** as **Send LDAP attributes as Claims** and click **Next**.



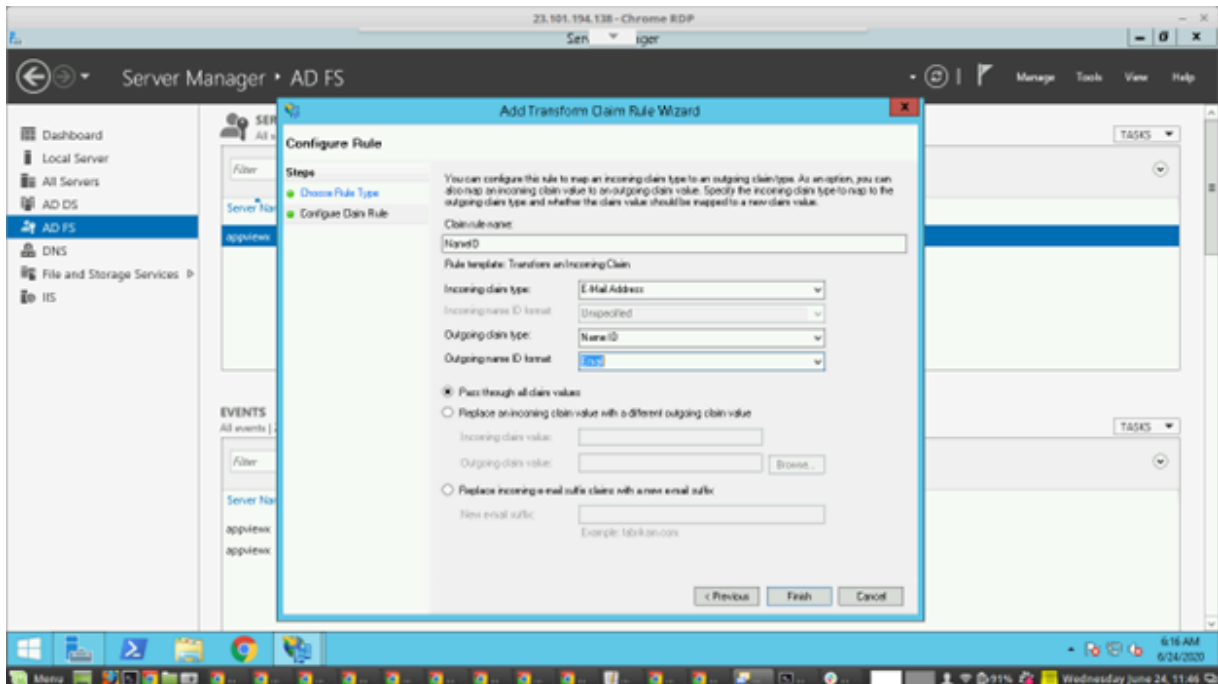
3. Enter a **Rule name** and select the **Attribute store** as **Active Directory**.
4. Enter the claim types as below and click **Finish**.
 Display-Name > FirstName, Surname > LastName, E-Mail-address > EmailId, Token-Groups-
 Unqualified Names > Roles, E-Mail-address > NameID, E-Mail-address > E-Mail-address.
5. Create another rule to transform the incoming claim by clicking **Add Rule > Rule Template** (Transform an Incoming Claim) and click **Next**.



6. Enter a **Rule Name** and select the **Incoming Claim Type** as **E-Mail-Address**, **Outgoing Claim Type** as **Name ID**, and **Outgoing Name ID Format** as **Email** and click **Finish**.

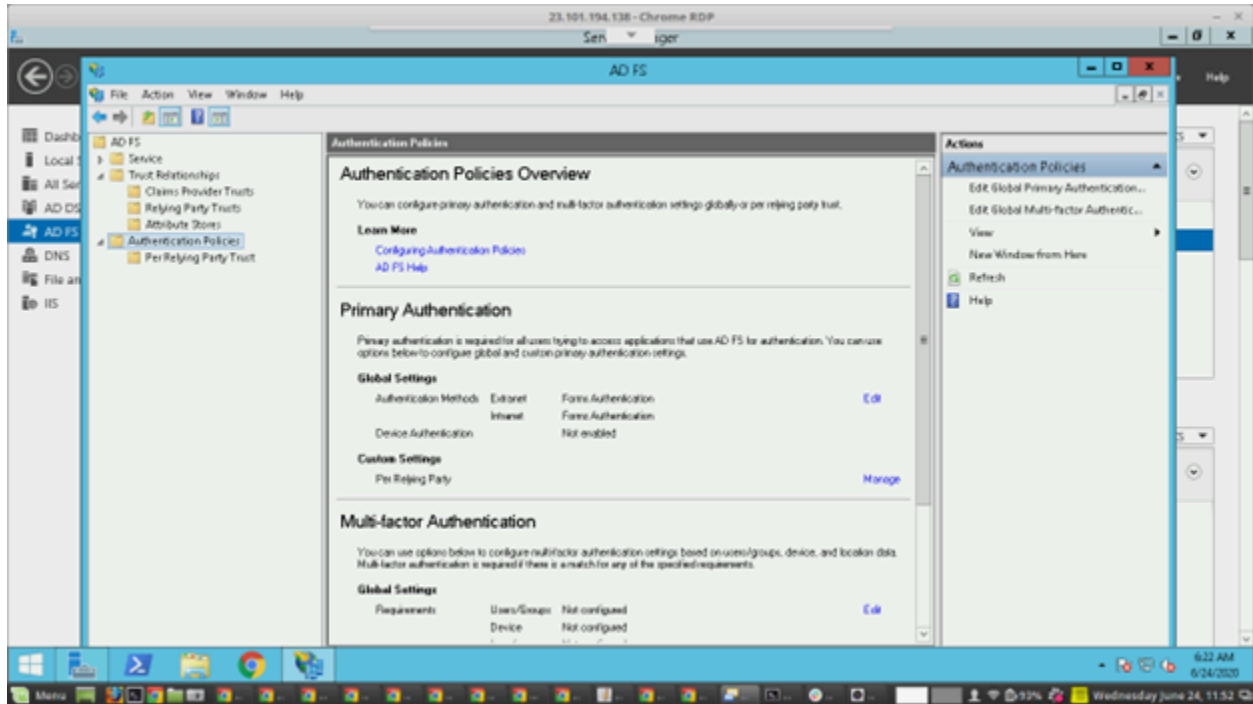


7. In the **Edit Claims** pane, click **Apply** and **OK**.



Enable Form-Based Authentication

For users to redirect from AppViewX to AD FS for authentication enable Form-based authentication as mentioned below. Under the AD FS menu > Authentication Policies the Primary Authentication should be Forms Authentication for Extranet and Intranet. If not select Edit and configure it as Forms Authentication.



Now AD FS is configured with all necessary details for SSO based authentication. To Export AD FS IDP metadata and upload in AppViewX SSO settings, export the metadata using the IDP URL and save it as an XML file.

Sample URL:

<https://appviewx.westus.cloudapp.azure.com/federationmetadata/2007-06/federationmetadata.xml>



Note: Role name passed in as a part of the SAML assertion should be configured in AppViewX on the Accounts > UserGroup and assign a role for accessing the application. For an IDP initiated SSO the following structure like URL should be used.

Sample IDP initiated URL: <https://appviewx.westus.cloudapp.azure.com/adfs/ls/idpinitiatedsignon>

Okta Integration

The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

Complete the following steps to begin the IDP configuration:

1. As an admin user or a user with the privilege to create an application, log in to the IDP and start creating the application.
2. Enter the basic details, name of the application, and logo update, if required.
3. Enter the configuration information of the service provider retrieved in the previous steps.
4. Enter the user attributes to be passed to AppViewX during the SAML assertion.
5. Download or copy the IDP metadata.
6. Map the Application to a user group or the user to the application.

1. Create an application.

The screenshot shows the 'Edit SAML Integration' page in the Okta admin console. The page has a blue header with the Okta logo and navigation links: Dashboard, Directory, Applications, Security, Roles, and Settings. On the right of the header is 'My Applications' with a plus icon. Below the header, the page title is 'Edit SAML Integration'. There are three tabs: '1 General Settings' (active), '2 Configure SAML', and '3 Feedback'. The 'General Settings' tab contains the following fields and options:

- App name:** A text input field containing 'AppViewX'.
- App logo (optional):** A section with a gear icon, a text input field, a 'Browse...' button, and an 'Upload Logo' button.
- App visibility:** Two checkboxes:
 - ☐ Do not display application icon to users
 - ☐ Do not display application icon in the Okta Mobile app

At the bottom of the form are 'Cancel' and 'Next' buttons. A yellow sidebar note on the right states: 'This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.'

2. Configure service provider details.

SAML Settings

GENERAL

Single sign on URL

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

3. Show Advanced Settings screen.

Response

Assertion Signature

Signature Algorithm

Digest Algorithm

Assertion Encryption

Enable Single Logout ☐ Allow application to initiate Single Logout

Authentication context class

Honor Force Authentication

SAML Issuer ID

4. Configure the User Attributes to be passed during the SAML assertion.

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Name	Name format (optional)	Value	
EmailId	Basic	user.email	×
FirstName	Basic	user.firstName	×
LastName	Basic	user.lastName	×
NameID	Basic	user.login	×
Mobile	Basic	000000	×

Add Another

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
Roles	Basic	Equals oktarole	×

Add Another

5. Finish the IDP configuration.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

☒ I'm an Okta customer adding an internal app
 ☐ I'm a software vendor. I'd like to integrate my app with Okta

i The optional questions below assist Okta Support in understanding your app integration.

App type **i**

☒ This is an internal app that we have created

Previous

Finish

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

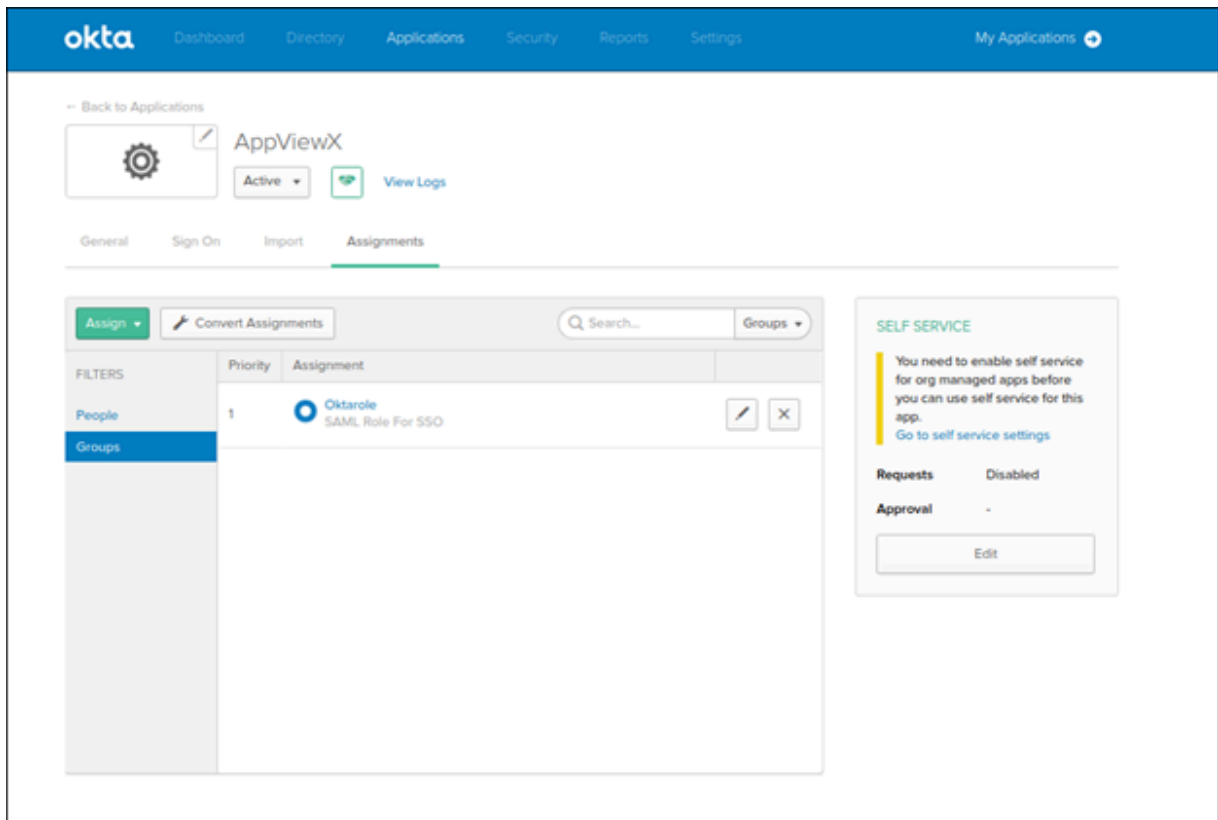
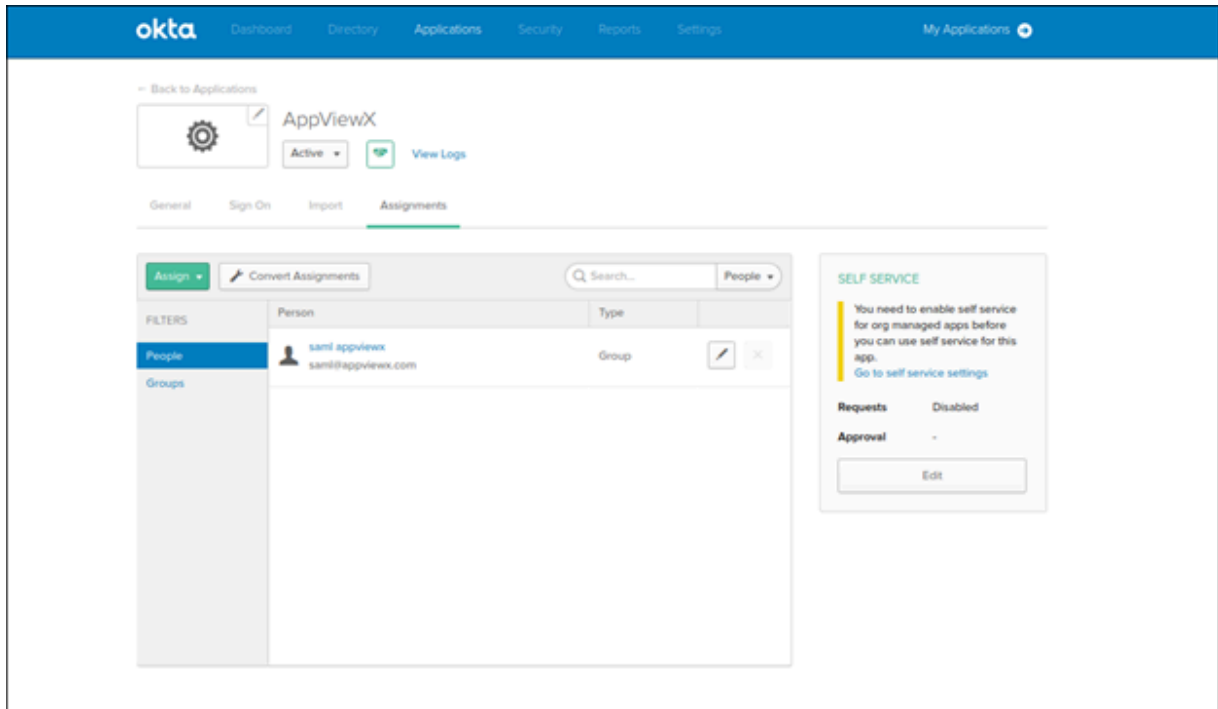
6. Click the View Setup Instructions in the Sign On tab.

Optional

Provide the following IDP metadata to your SP provider.

```
<?xml version='1.0' encoding='UTF-8'?><md:EntityDescriptor xmlns:md='urn:oasis:names.tc:SAML:2.0:metadata'  
xsi:type='http://www.okta.com/xsd9/y6y7dIdqkSM356?'><md:IDPSODescriptor WantAuthnRequestsSigned='false'  
protocolSupportEnumeration='urn:oasis:names.tc:SAML:2.0:protocol'><md:KeyDescriptor use='signing'><ds:KeyInfo  
xmlns:ds='http://www.w3.org/2000/09/xmldsig#'><ds:X509Data>  
<ds:X509Certificate>MIIgDCCApCgAwIBAgI/GAIWodnVYMAOGCSqGSIb3DQEBCwUAMIGUMQswCYDDVOQGGEwJVZUEtMBEG  
AUIECawKQzFsaZWcmSpYTEWMBOGAUIEBwwNU2FuEZYyWJaXNjbzENMAcGAUIECgwETJIOYTTEU  
MIIGAIAUCwwLUINPUHjvdmklZXlxFATBtbNVBAMMDGFwcHZpZXdl4LNzbzEcMBoGCsgSib3DQEIJ  
ARYNAUYCbmbObva3RhRmlNbvtAEfWoxOTAYMEDEwOTQOMJAfaWoYOTAYMEDEwOTQSMJAaIMIGUMQswCYDD  
VQQGEwJVZUEtMBEGAUIECawKQzFsaZWcmSpYTEWMBOGAUIEBwwNU2FuEZYyWJaXNjbzENMAcGA  
AUIECgwETJIOYTTEUUMBAGAUIECwwLUINPUHjvdmklZXlxFATBtbNVBAMMDGFwcHZpZXdl4LNzbzEc  
MBoGCsgSib3DQEJARYNWA5bmOBva3RhRmlNbvtCCAASoDGYYKoZhivCAQEBAQAAGggEPADCCAAQC  
ggEBAIC2ziRCr7gbMVcyYrRkJDLGRwaUlzhQkvTWVoEZdbik/KTHavVMXPghNinkOhUcxzfzHePFBIwx  
9JEThInvvHVlg6ZktYotRGDFFOFIhxzhfwegR5yt27hiu/VteGT8GNcwOoyzdJdrDuZg27yl  
jiqGPKR/Liwrot54RLIP2VCImOFdiOWWiOOUnISIEFnAd+2UECZZLOogJKDPfcDisuhmg5btTKUS  
TlpIxarNeach2kiRI4feeqOdVgaighgs+zMN44iz+YGsbuELEIKerOabEtYITJmsVmqEcs8FUvkx  
LLdzEvPhh89vOmUJIZigTJIPI9N+NEUzyJsHgqmUCAwEAATANBgkqhkiG9w0BAQsFAAQCAQEA  
Ro42XhgDe3dx9ntXKr2ULtoitQeVoFdskUljla2zDRcvHis2OvfWCWW-QdUehSuUlljGXbaHa  
cGLEAJvuOlakEKymUDKGAOjdL7lbwTK69fz19F7pt6bsqs8yj5IOavitN3NilzZdkRPip1  
hnKcjOSVyMP/ba7DXOXODzoZjp+pWjoClpa4EI9KOXWkgKSJS83ou/WxtOc4Jak4/YueafYbnHf  
amyEf6w96QM6scEGLCxxZbozc57BMZOM4Mr6zXOTS8puAX6NBndNkdwoQ9JSeXM3U6IRWv59jet
```

Copyright © 2023 [AppViewX, Inc]. All Rights Reserved.



9. Browse and upload the IDP metadata to AppViewX. Then, click Save.

LDAP TACACS RADIUS **SAML** Order

SSO Information

SSO ☒

Meta data **Browse** ⓘ

* Issuer URL ⓘ

* SSO URL ⓘ

SLO ☐

SLO URL ⓘ

* Upload certificate **Browse**

Save **Cancel**

Forgerock Integration

1. Login to the Forgerock IDP intense / console.

← → ↻ ⚙ Not secure | openam.try.appviewx.com:8080/openam/XUI/#login/

FORGEROCK

SIGN IN

User Name

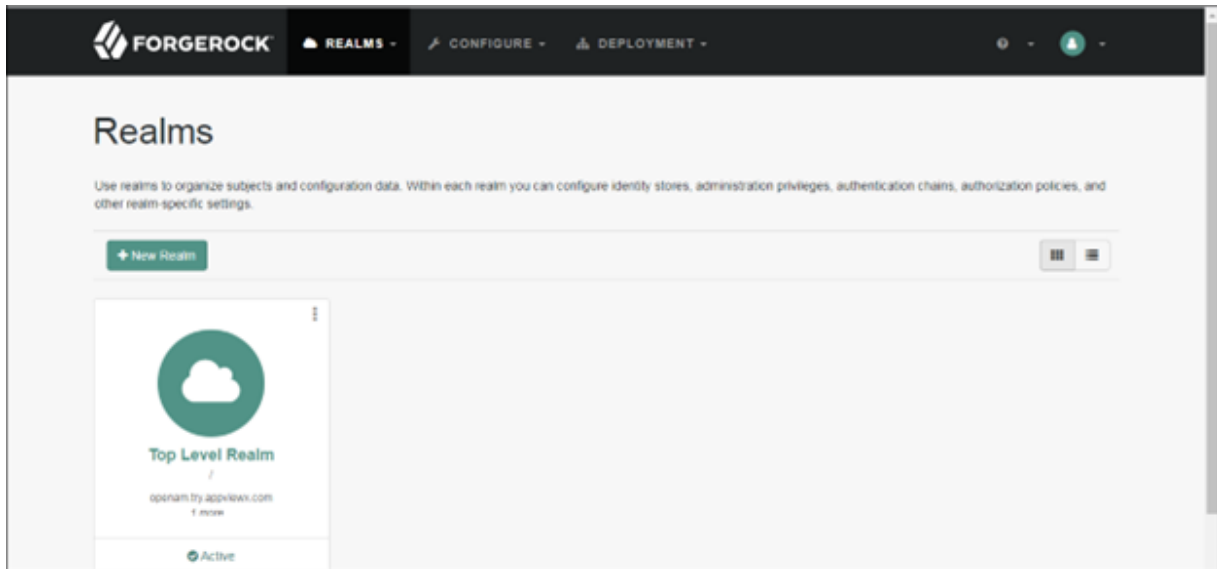
Password

☐ Remember my username

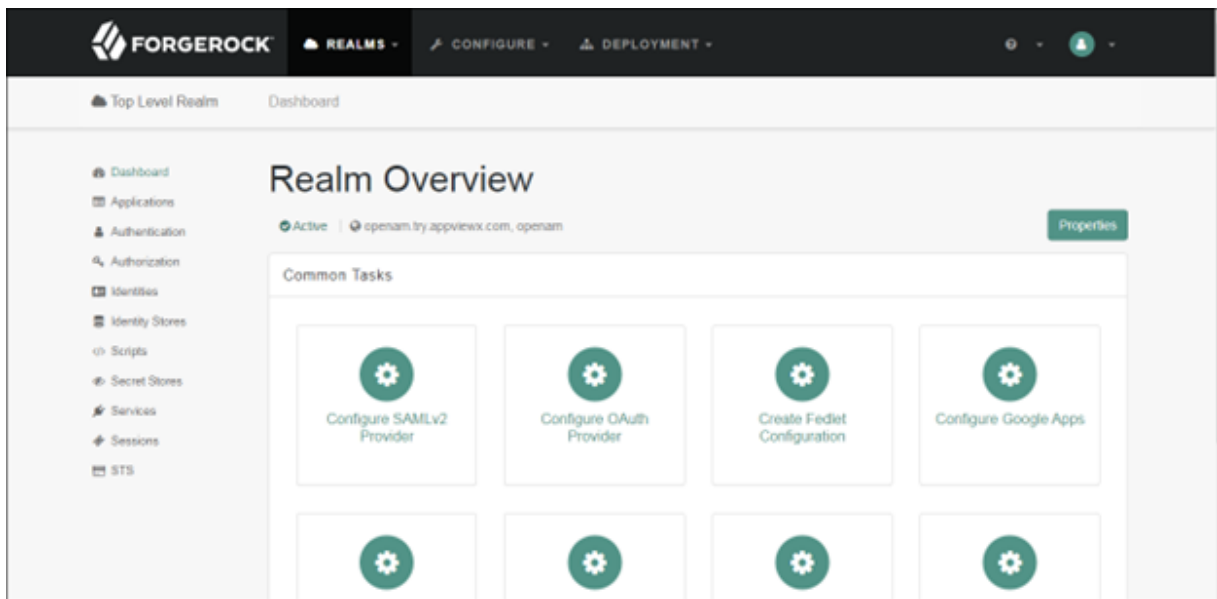
LOG IN

Copyright © 2016-2019 ForgeRock AS. All rights reserved.

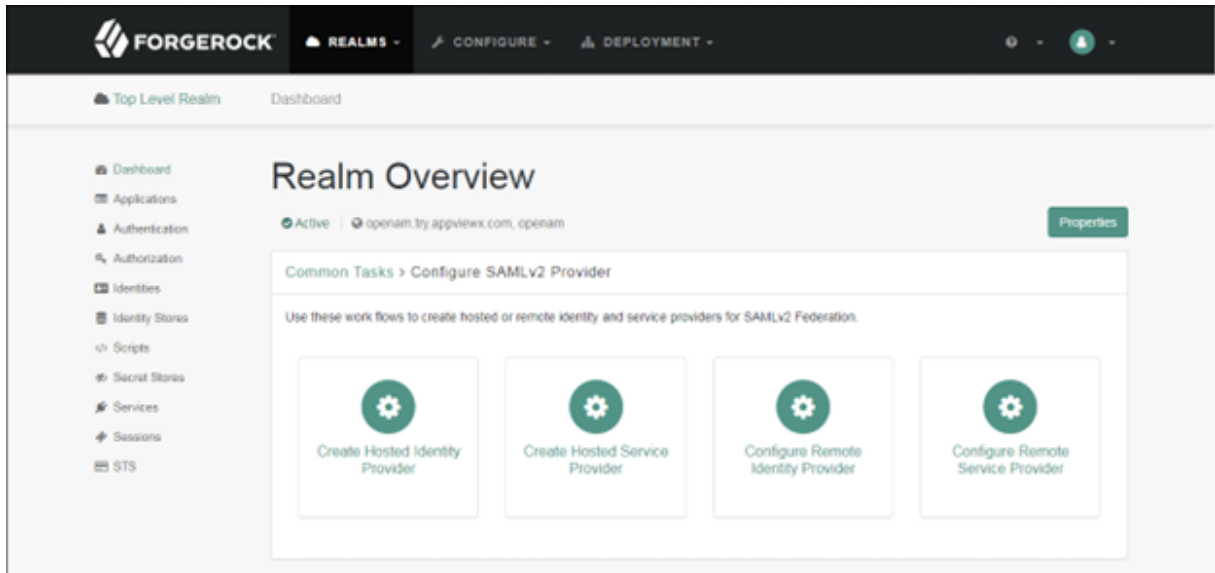
2. Select the respective Realm.



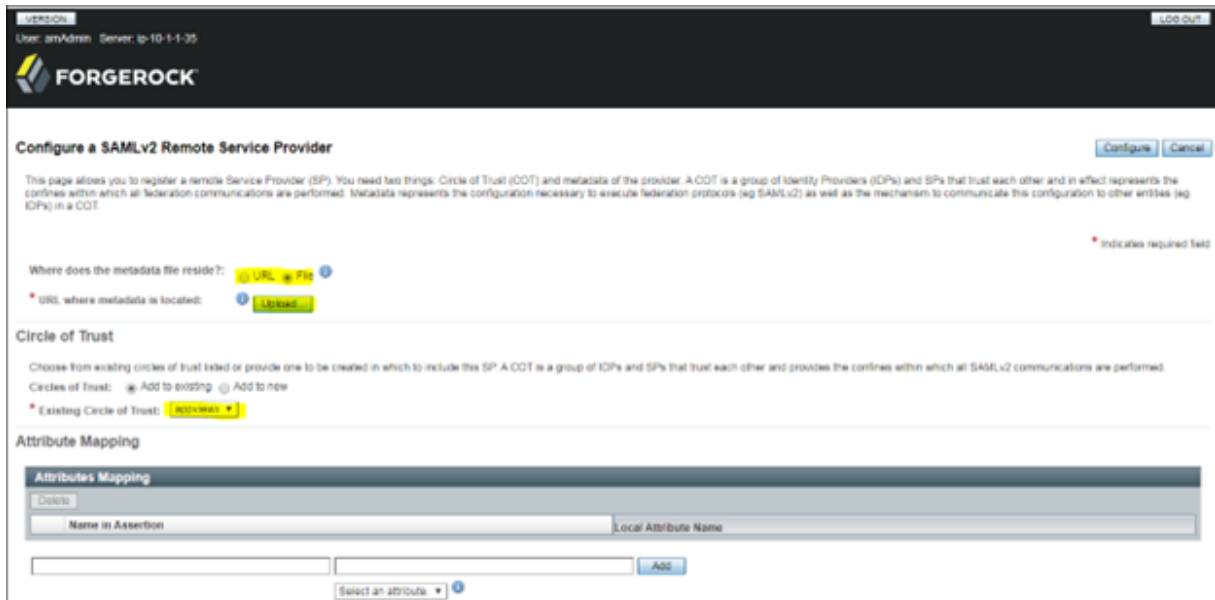
3. Under **Common Tasks**, select **Configure SAML v2 provider**.



4. For Configuring AppViewX configuration, select **Configure Remote Service Provider**.



5. For metadata upload, select the **File** option and select/create the circle of trust for mapping AppViewX to the IDP and click **Upload**.



6. Upload the AppViewX metadata which was downloaded earlier and click **Configure** to save the settings.

Configure a SAMLv2 Remote Service Provider

This page allows you to register a remote Service Provider (SP). You need two things: Circle of Trust (COT) and metadata of the provider. A COT is a group of Identity Providers (IDPs) and SPs that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg IDPs) in a COT.

Where does the metadata file reside?: ☐ URL ☒ File

* URL where metadata is located:

Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this SP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.

Circles of Trust: ☒ Add to existing ☐ Add to new

* Existing Circle of Trust:

Attribute Mapping

Name in Assertion	Local Attribute Name

The page will redirect to the common tasks under the specific realm.

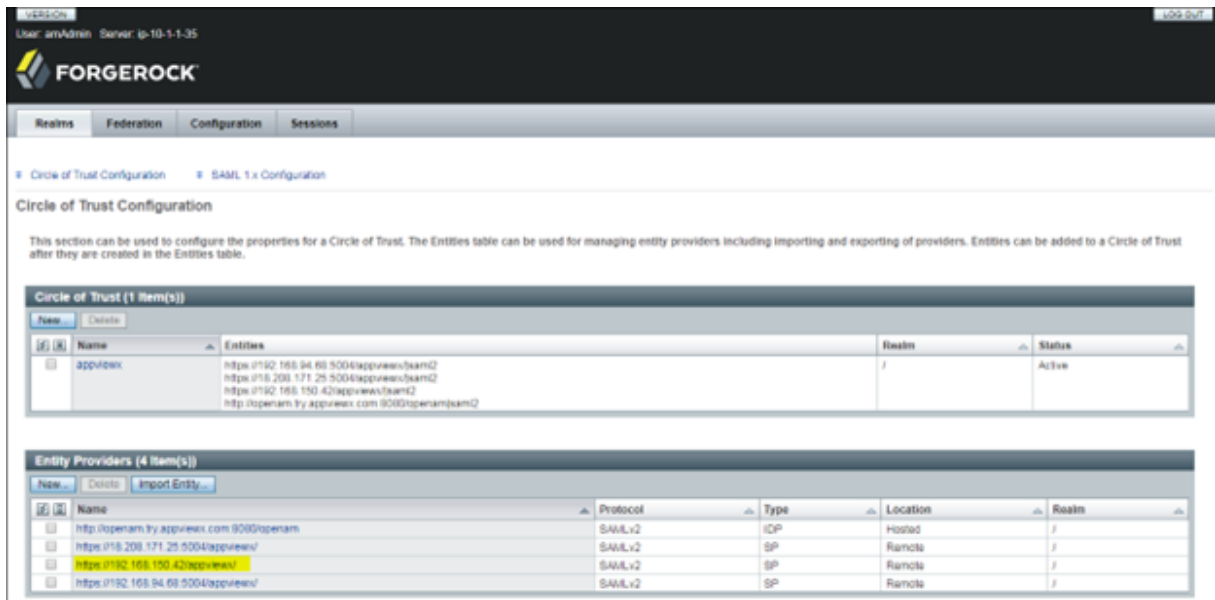
7. Access **Applications** > **Federation** from the left navigation pane.

Federation

Entity Providers

NAME	ENTITIES	STATUS
☐ appviewx	https://192.168.94.68:5004/appviewx/saml2 https://192.208.171.25:5004/appviewx/saml2 http://openam.try-app-viewx.com:9080/openam https://192.168.142.184:5004/appviewx/saml2	Active

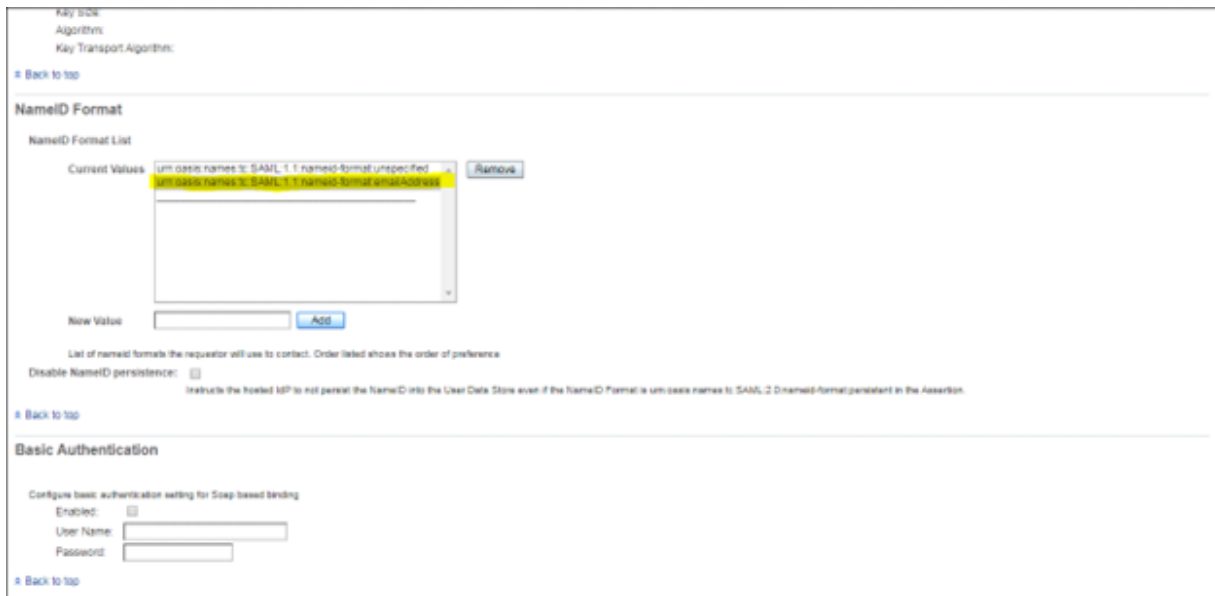
8. Select the entity providers tab.



This will redirect to the Federation tab with the list of Service providers and IDP configuration.

9. Select the respective Entity ID to navigate to the settings of the respective entity configuration.
10. On the **Assertion Content** tab, add the following in the NameID Format and click **Save** on the top right.

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress



11. On the **Assertion Processing** tab, add the below assertion parameter which has to be passed as a part of the SAML assertion and click **Save**.

EmailId=mail ; FirstName=cn ; LastName=sn ; NameID=mail ; Roles=isMemberOfAuthentication.

SP

Assertion Content Assertion Processing Services Advanced

https://192.168.150.42/appviewx/ Save Reset Back

Attribute Mapper

Attribute Map

Current Values: Email=mail, FirstName=on, LastName=on, Name=on, Roles=memberOf Remove

New Value: Add

This mapping is the configuration used by the Attribute Mapper. Mapping should be defined as SAML_ATTRIBUTE_NAME=PROFILE_ATTRIBUTE_NAME in assertion. Example: EmailAddress=mail, Address=postalAddress.

Back to top

Artifact Message Encoding

Encoding: UTF-8

Back to top

Save Reset Back

12. Modify IDP configuration to accept a password-based Authentication Context.

13. Navigate to **Applications > Federation** and select Entity Provider TAB.

FORGEROCK REALMS CONFIGURE DEPLOYMENT

Top Level Realm Applications - Federation

Dashboard Applications Agents Federation OAuth 2.0 Authentication Authorization Identities Identity Stores Scripts Secret Stores Services Sessions STS

Federation

Circles of Trust Entity Providers

+ Add Circle of Trust Delete

NAME	ENTITIES	STATUS
appviewx	https://192.168.94.68:5004/appviewx/saml https://18.208.171.25:5004/appviewx/saml http://openam.try-appviewx.com:8080/openam https://192.168.142.184:5004/appviewx/saml	Active

14. Under the **Federation** tab, select the IDP config under **Entity Providers**.

User: amAdmin Server: 10-1-1-35

FORGEROCK

Realms Federation Configuration Sessions

Circle of Trust Configuration SAML 1.x Configuration

Circle of Trust Configuration

This section can be used to configure the properties for a Circle of Trust. The Entities table can be used for managing entity providers including importing and exporting of providers. Entities can be added to a Circle of Trust after they are created in the Entities table.

Circle of Trust (1 Item(s))

Name	Entities	Realm	Status
appviewx	https://192.168.94.68:5004/appviewx/saml2 https://16.208.171.25:5004/appviewx/saml2 https://192.168.150.42/appviewx/saml2 http://openam.ry.appviewx.com:8080/openamsaml2	/	Active

Entity Providers (4 Item(s))

Name	Protocol	Type	Location	Realm
http://openam.ry.appviewx.com:8080/openam/	SAMLv2	IDP	Hosted	/
https://16.208.171.25:5004/appviewx/	SAMLv2	SP	Remote	/
https://192.168.150.42/appviewx/	SAMLv2	SP	Remote	/
https://192.168.94.68:5004/appviewx/	SAMLv2	SP	Remote	/

15. Under the **Authentication Context** section, check the Password-based context.

Authentication Context

Mapper:

* Default Authentication Context:

Authentication Context (25 Item(s))

Supported	Context Reference	Key	Value	Level
☐	InternetProtocol	None		0
☐	InternetProtocol/Password	None		0
☐	Kerberos	None		0
☐	MobileOneFactorUnregistered	None		0
☐	MobileTwoFactorUnregistered	None		0
☐	MobileOneFactorContract	None		0
☐	MobileTwoFactorContract	None		0
☒	Password	None		0
☒	PasswordProtectedTransport	None		0
☐	PreviousSession	None		0
☐	X.509	None		0
☐	PGP	None		0
☐	SPN	None		0
☐	XMLDSig	None		0
☐	Smartcard	None		0
☐	SmartcardPKI	None		0
☐	SoftwarePKI	None		0
☐	Telephony	None		0
☐	NomadicTelephony	None		0
☐	PersonalTelephony	None		0

16. Above the Context, add the NameID Value Map and save the settings.

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=mail.

[Back to top](#)

NameID Format

NameID Format List

Current Values: [Remove](#)

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient
- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
- urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
- urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
- urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

New Value: [Add](#)

List of nameid formats the requestor will use to contact. Order listed shows the order of preference

NameID Value Map

Current Values: [Remove](#)

- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress@mail
- urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName=
- urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName=
- urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos=
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified@mail

New Value: [Add](#)

Defines mapping between the NameID format and user's profile attribute. Example urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress@mail or urn:oasis:names:tc:SAML:2.0:nameid-format:persistent/objectGUID:binary. If the defined NameID format is used in protocol, the profile attribute value will be used as NameID value for the format in the Subject. The binary flag can be used to indicate that the profile attribute is binary and should be Base64 encoded when used as the NameID value.

[Back to top](#)

- Now access AppViewX with the SSO authentication with Forgerock.
- Export IDP metadata and upload it in AppViewX SSO settings. To export metadata using the IDP URL and save it as an XML file. **Sample URL:** `http://openam.try.appviewx.com:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://openam.try.appviewx.com:8080/openam`



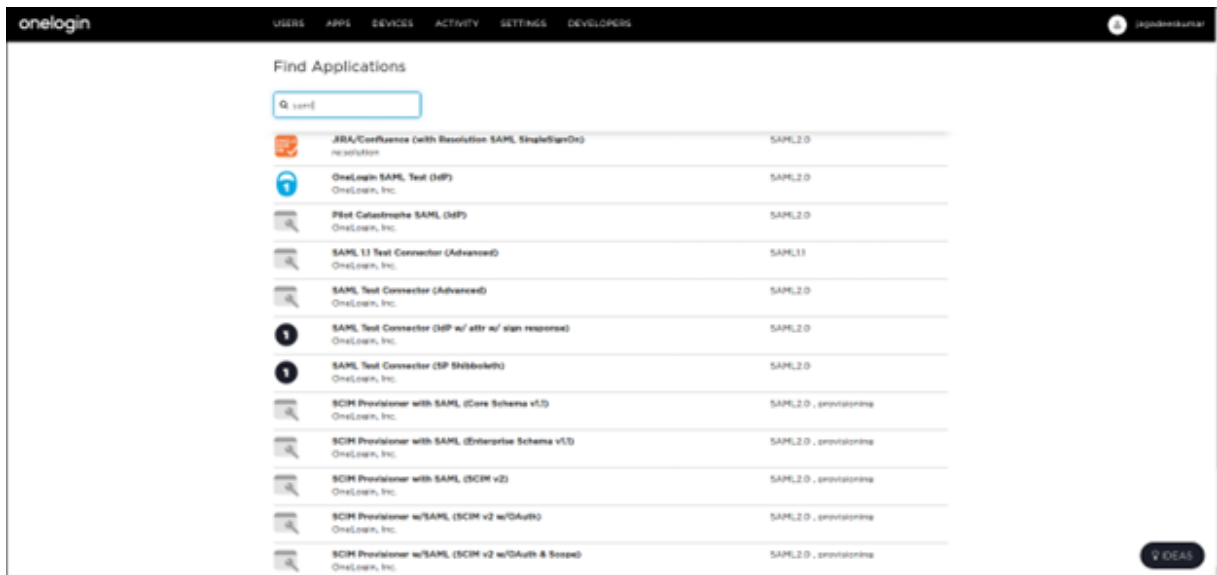
Note: Role name passed in as a part of the SAML assertion should be configured in appviewx on the Accounts > UserGroup and assign a role for accessing the application. For an IDP initiated SSO the following structure like URL should be used. **Sample IDP initiated URL:**
`http://openam.try.appviewx.com:8080/openam/idpssoinit?metaAlias=/idp&spEntityID=https://192.168.x.x:31443/appviewx/`

OneLogin Integration

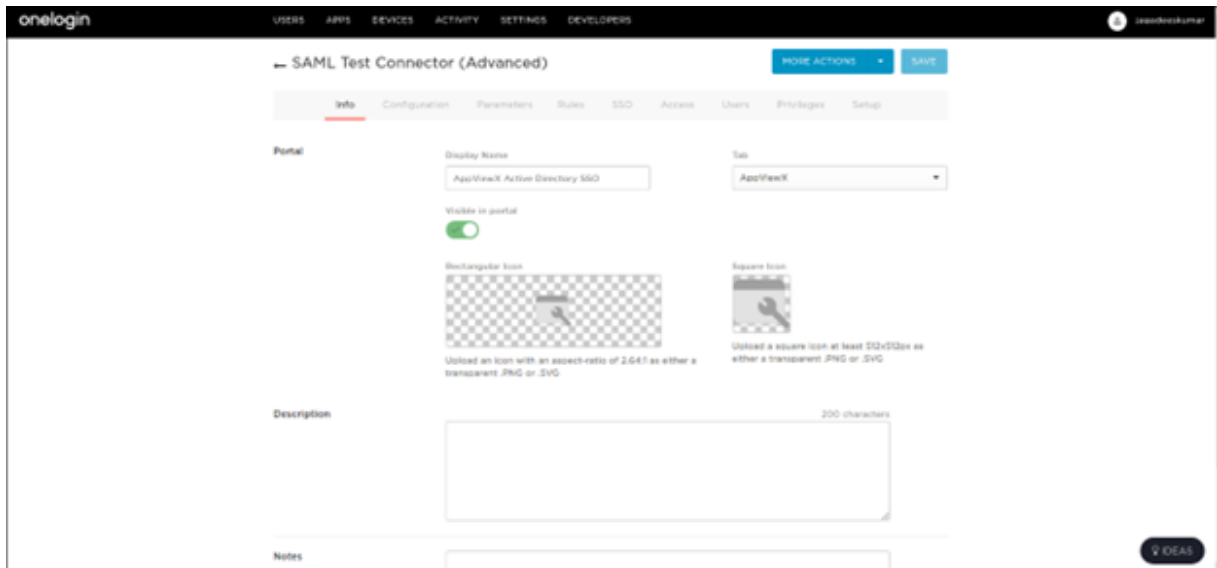
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

The following are the steps to configure AppViewX SAML attributes in OneLogin.

1. Create a new application. Click Add application and search for SAML Test Connector.



2. Provide the application name and application details of AppViewX on the information page.



3. **AppViewX SAML attributes:** On the Configuration tab, provide the ACS consumer URL, single login URL, and single logout URL. This can be fetched by navigating to AppViewX > Settings > General > Authentication > SAML > Enable SSO > Service URL from the configuration found at the end of the page and specify the remaining settings to default.

onelogin

USERSAPPSDEVICESACTIVITYSETTINGSDEVELOPERS

jagadeeskumar

← SAML Test Connector (Advanced)

MORE ACTIONS

SAVE

InfoConfigurationParametersRulesSSOAccessUsersPrivilegesSetup

Application Details

RelayState

Audience

Recipient

ACS (Consumer) URL Validator*

https://192.168.96.121:5004/appviewx/ssoLo;

*Required.

ACS (Consumer) URL*

https://192.168.96.121:5004/appviewx/ssoLo;

*Required

Single Logout URL

https://192.168.96.121:5004/appviewx/ssoLo;

Login URL

Only required if you select Service Provider as the SAML Initiator.

SAML not valid before

3

* Required - Specifies time period, in minutes, the assertion is valid for.

SAML not valid on or after

3

* Required - Specifies time period, in minutes, the assertion is valid for.

SAML initiator

OneLogin

SAML nameID format

Email

SAML issuer type

Specific

SAML signature element

Response

Encrypt assertion

☐

SAML encryption method

TRIPLEDES-CBC

Generate AttributeValue tag for empty values

☐

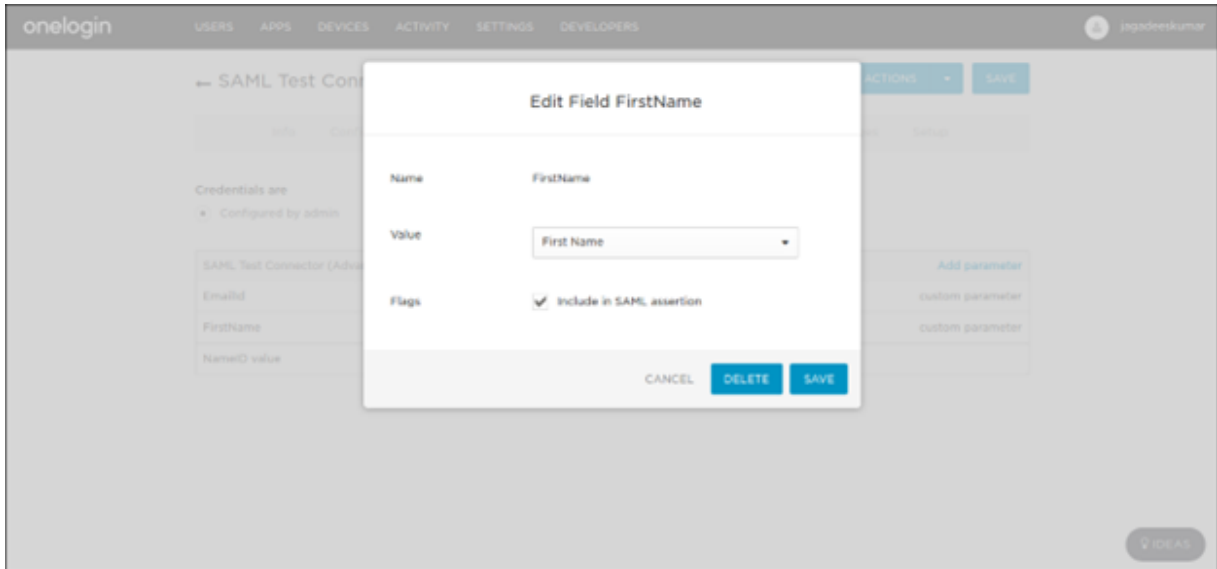
SAML sessionNotOnOrAfter

1440

Specifies the time period, in minutes, the session is valid for. Default is 1440 minutes (24 Hours).

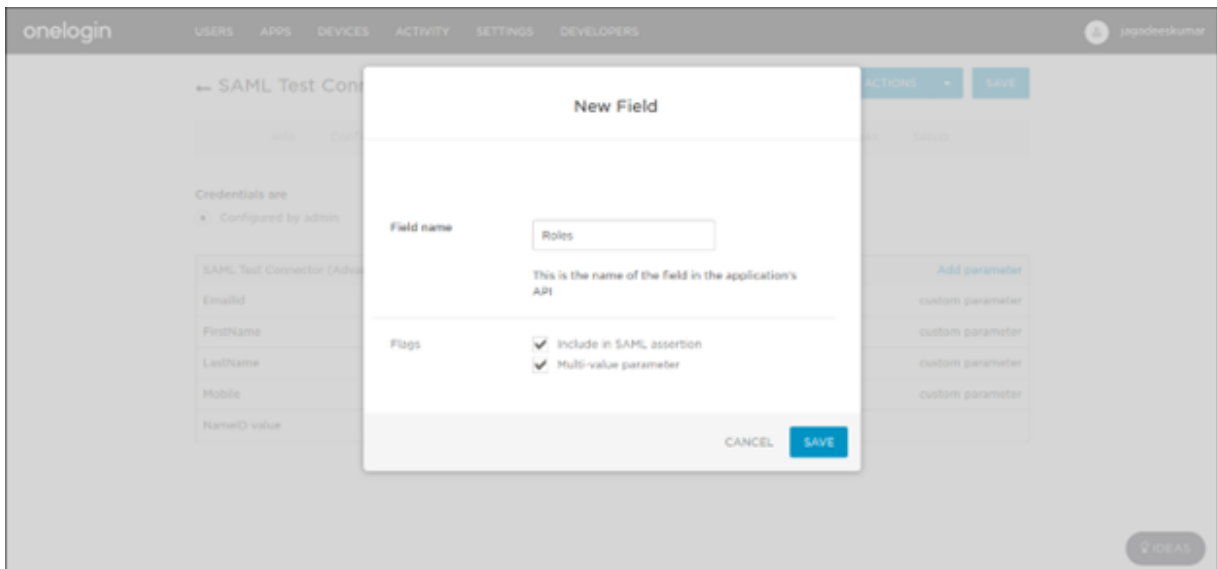
IDEAS

4. **Parameters to be sent to AppViewX:** The following parameters are samples that have been sent to AppViewX. Create a parameter called FirstName which sends the user's first name to AppViewX in the SAML Assertion.

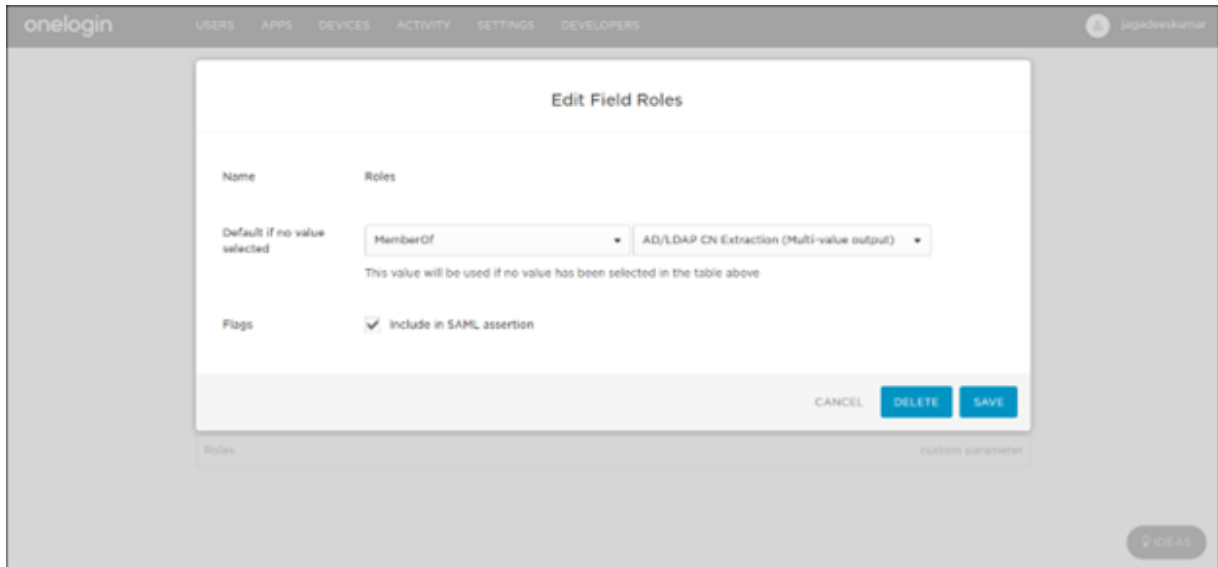


Include the flag in SAML Assertion for all the added parameters.

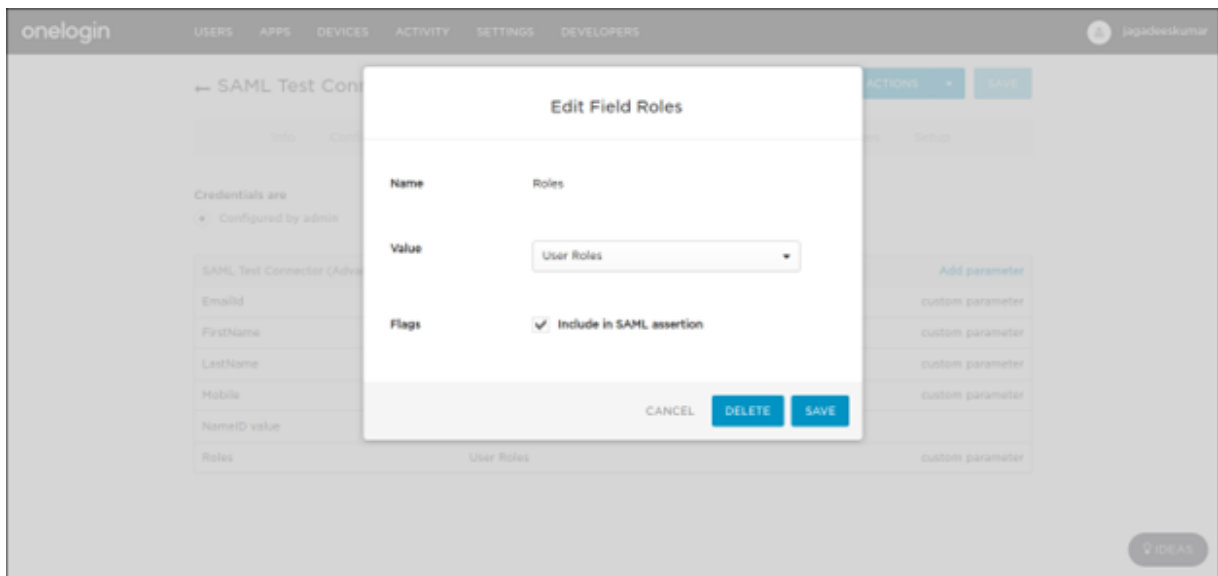
5. **Sending User Groups to AppViewX:** To send User Groups to AppViewX from OneLogin through SAML Assertion, the following configuration has to be performed. OneLogin should be integrated with the Active Directory. Provide the field name as Roles and enable the Flags SAML assertion and multi-value parameter.



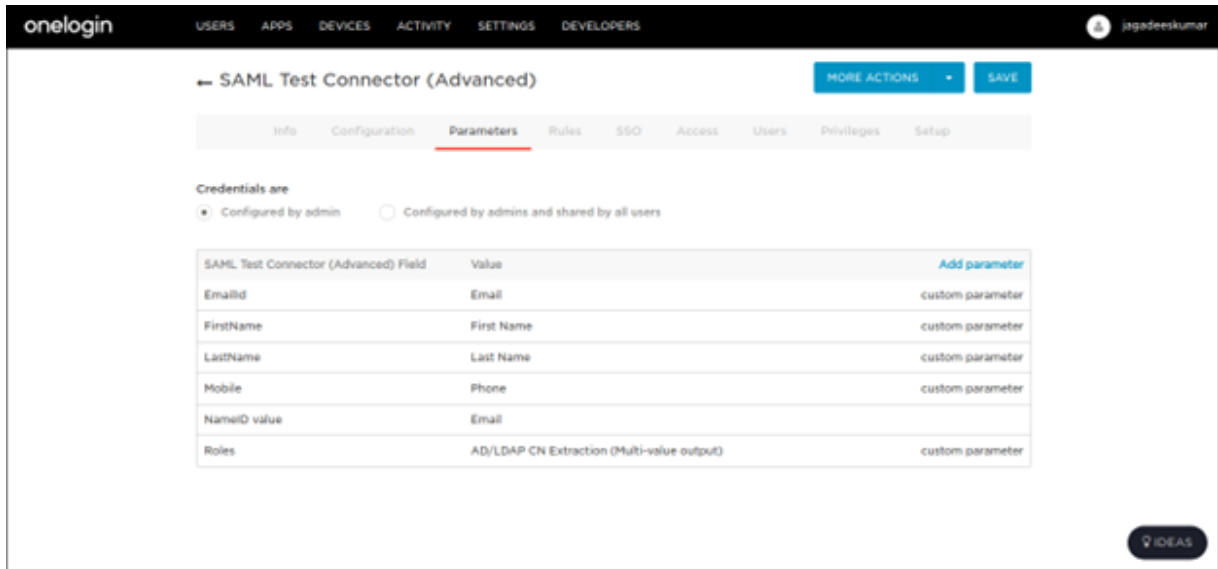
6. To pass the respective user's MemberOf attribute as Role, provide the field name as MemberOf and select the AD/LDAP CN Extractor.



OneLogin without AD integration: Pass the roles field with user roles as value.



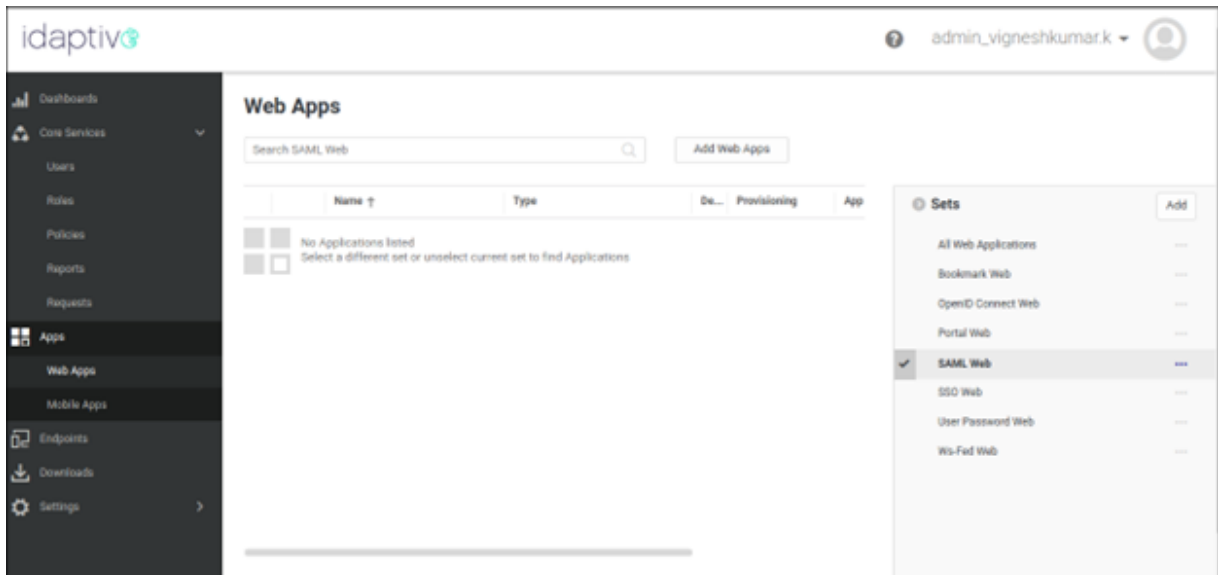
- Other parameters that have to be passed:** The following parameters have to be passed to AppViewX through the SAML assertion.



8. **Assign application to User and Role:** Once the federation metadata is downloaded, click Save. Create the UserGroup under Roles in the Administration section. The created application is then assigned to the user group and the synced users will be added to it.

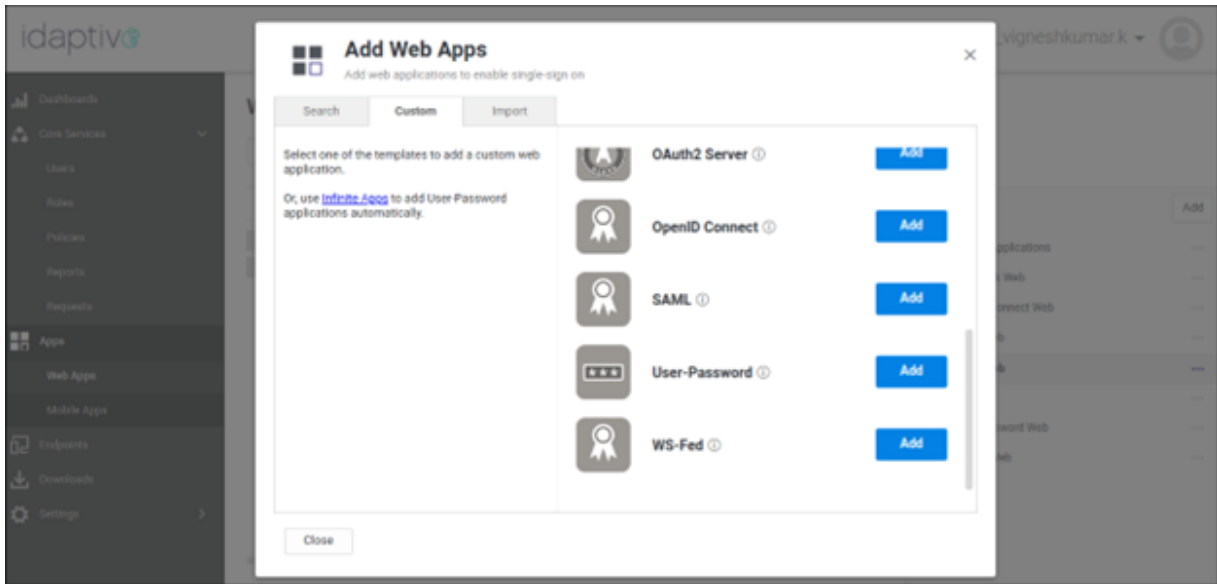
Idaptive Integration

1. Login to the Idaptive SSO platform.
2. Navigate to **Apps > WebApps > Select SAML Web**.
3. Select **SAML Web**.



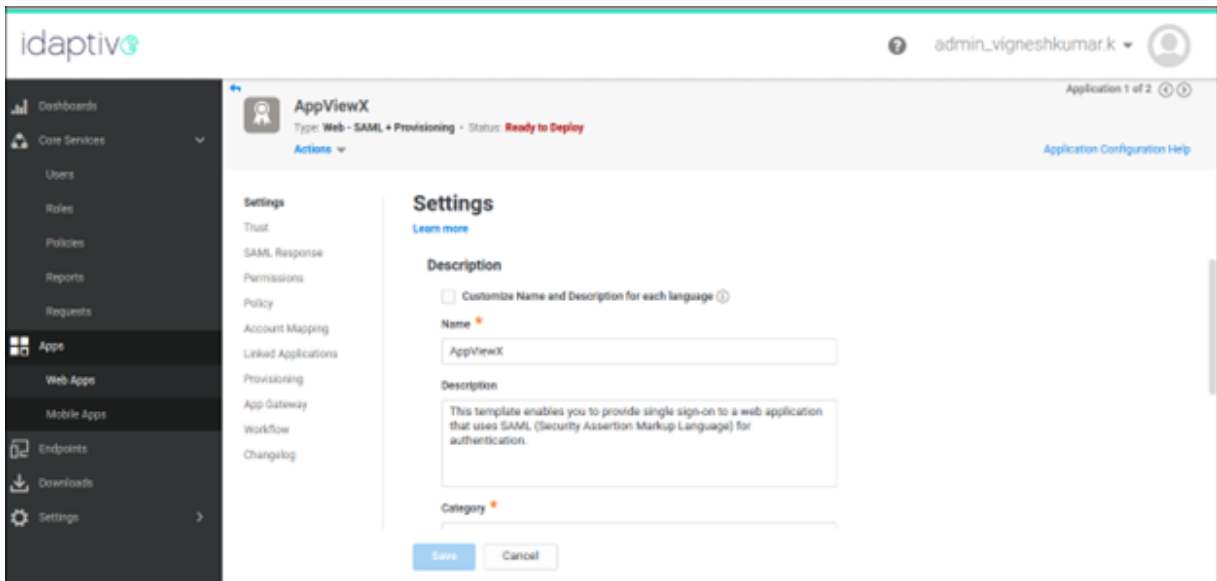
4. Click **Add Web Apps**.

5. In the **Add Web Apps** window, under the **Custom** tab, click **Add** for **SAML**.

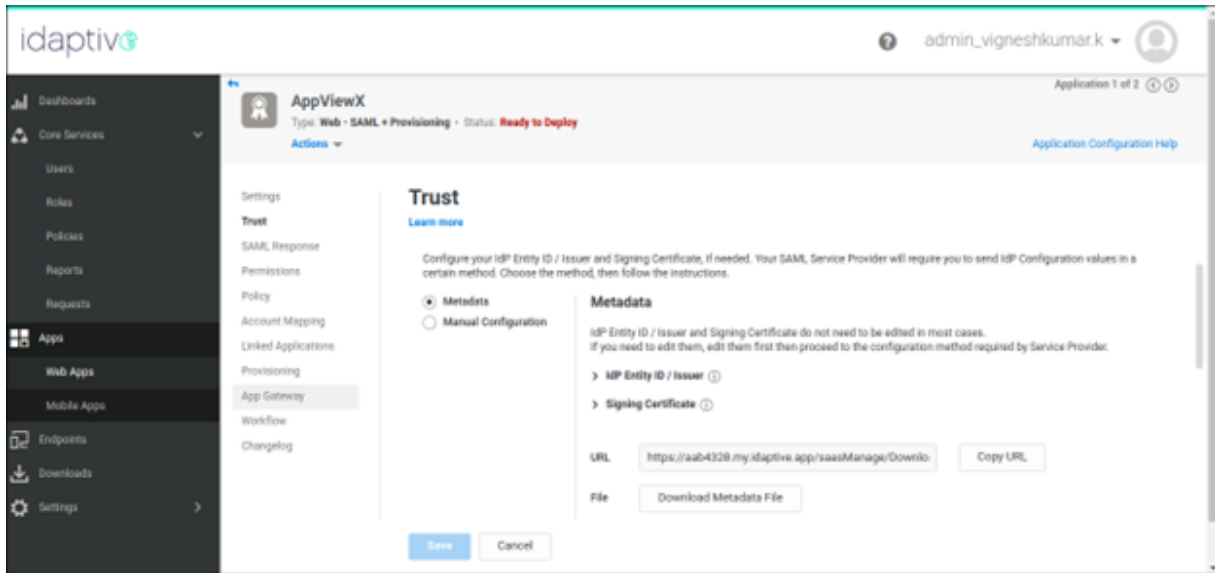


SAML app is added to the Web Apps Inventory.

6. Select the SAML app in the Web Apps Inventory and proceed with the configuration.
7. In the **Settings** tab, enter the name for the app as **AppViewX** and save the configuration.

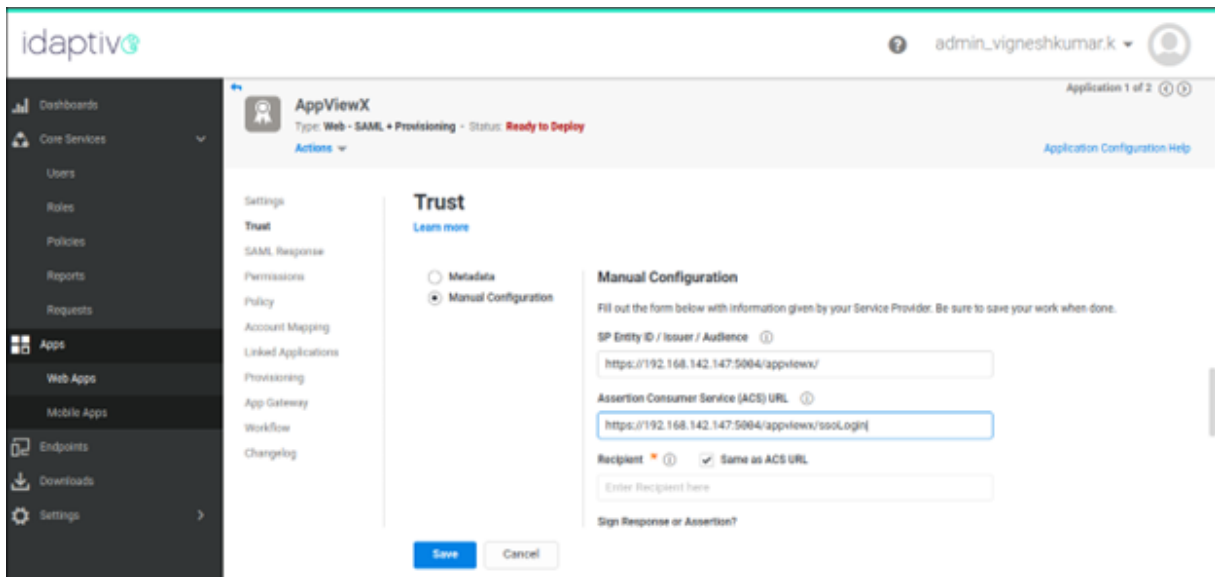


8. In the **Trust** tab, click **Download Metadata File**.



9. Select the **Manual Configuration** option.

10. Copy and paste the Entity ID URL from AppViewX on the SP Entity ID field in Idaptive portal and the Service URL from AppViewX on the ACS URL field in the Idaptive portal.



11. Check if the Recipient checkbox is the same compared to the ACS URL. Leave the rest of the settings to default. Configure the Single Logout URL field with the value copied from the SLO URL in AppViewX. **Save** the config.

The screenshot shows the 'Trust' configuration page for 'AppViewX' in the idaptive console. The left sidebar contains navigation links for Dashboards, Core Services, Users, Roles, Policies, Reports, Requests, Apps, Web Apps, Mobile Apps, Endpoints, Downloads, and Settings. The main content area is titled 'Trust' and includes a 'Learn more' link. Below the title, there are several configuration fields: 'Single Logout URL' with the value 'https://192.168.142.147:5004/appviewx/logout', 'Encrypt SAML Response Assertion' (unchecked), 'Relay State' (empty), and 'Authentication Context Class' (set to 'unspecified'). There are 'Save' and 'Cancel' buttons at the bottom.

12. In the **SAML response** tab, add the below assertion attributes with the same format.
 FirstName > LoginUser.FirstName, LastName > LoginUser.LastName, NameID > LoginUser.Email,
 EmailId > LoginUser.Email, Roles > LoginUser.RoleNames (This should be the user associated User
 Groups / Security Groups).

The screenshot shows the 'SAML Response' configuration page for 'AppViewX' in the idaptive console. The left sidebar is the same as the previous screenshot. The main content area is titled 'SAML Response' and includes a 'Learn more' link. Below the title, there is a text box explaining the purpose of the configuration and an 'Add' button. A table with two columns, 'Attribute Name' and 'Attribute Value', contains the following mappings:

Attribute Name	Attribute Value
☐ / FirstName	/ LoginUser.FirstName
☐ / LastName	/ LoginUser.LastName
☐ / NameID	/ LoginUser.Email
☐ / EmailId	/ LoginUser.Email
☐ / Roles	/ LoginUser.RoleNames

There are 'Save' and 'Cancel' buttons at the bottom.

13. Click **Save**.
14. Assign the application to the respective Role and the Role to the respective Users. Once done
 configure the same Role in AppViewX in the **Account > User Group** module and assign respective
 AppViewX Role permission to the User Group.
15. Now access AppViewX with the help of External login using SAML.

OpenID Connect- Overview

OpenID Connect (OIDC) is an identity layer built on top of the OAuth protocol, which provides a modern and intuitive Single Sign-on (SSO) experience for you and your end-users. For example, administrators can configure Single Sign-on with a third-party identity provider that supports OpenID Connect. Users then have the option to log in to the application using their identity provider credentials.

- [AppViewX Integration with OIDC Provider](#)
- [Login Workflow](#)
- [Steps to Integrate OIDC](#)

Before you begin

- Register AppViewX as an OIDC application with your Identity Provider (IdP) and note the Client ID, Client Secret, and Well-known configuration URL.
- The OIDC entity profile must be an authorization code grant type.
- Enable SSO with Authentication Protocol as OIDC in AppViewX.
- Role required: admin
- OIDC based SSO is supported from AppViewX release 21.1.X and above.

AppViewX Integration with OIDC Provider

To integrate AppViewX with OIDC provider, follow the below steps:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, turn on the **Enable SSO** toggle.
The **Authentication Protocol** options are displayed.
3. Select **OIDc** as the **Authentication Protocol**.
The **Service Provider Information** section will be auto-populated based on the OIDC selection.
4. Copy the Callback and SLO URL, which is to be configured at the OIDC identity provider settings for AppViewX, from the **Service Provider Information** section.

LDAP
TACACS
RADIUS
SSO
IP Restriction
Authentication settings
OAuth Settings

Enable SSO ☒

* Authentication Protocol ☐ SAML ☒ OIDC

Service Provider Information

Data center

* Appviewx Host ⓘ

Callback URL ⓘ

SLO URL ⓘ

ⓘ Register AppViewX as a client in OIDC provider with the Callback URL and Logout URL ,then configure this setting with Client details.

5. Under the IDP Configuration section enter the required field information.

IDP Configuration

Client Name * ⓘ

Client ID * ⓘ

Client Secret * ⓘ

Discovery Endpoint (Well Known) URL * ⓘ

Fetch details ⓘ

ⓘ Required OIDC provider details are fetched successfully. [View Details](#)

The following table describes the field information in this section:

Field	Description
*Client Name	Unique name for the OIDC identity provider configuration.
*Client ID	The client ID of the application that is registered in the third-party OIDC identity provider.

Field	Description
*Client Secret	The client secret of the application that is registered in the third-party OIDC identity provider.
*Discovery Endpoint (Well known) URL	The URL contains metadata about the third-party OIDC identity provider.
All * marked fields are mandatory.	

6. Under the **Advanced** section, turn the **Local Authorization** toggle on/off to define custom claim mapping based on the ID claims which are sent from the OIDC Identity provider.

Turn the **Local Authorization** toggle **on** to define the following privileges:

- When a user from an OIDC provider tries to log in to AppViewX for the first time, the user account will be created under Account > User within AppViewX. But users will not be allowed to perform any operations until Admin assigns the user to the respective User Group.
- To enable the user with a successful login, an User Group must be created as a prerequisite, and the User Group must be assigned with Roles and Resources permissions for the SSO users and has to be assigned within AppViewX by mapping the users to the User Group.

Turn the **Local Authorization** toggle **off** to define the following privileges:

- When a user from an OIDC provider tries to log in to AppViewX, with Local Authorization disabled it is assumed that the Security Groups are passed as a part of the ID token.
- Create the required Security Group under the Menu > Account > User Groups within AppViewX by assigning respective Roles and Resources.

7. Under the **Advanced** section, enter the API Key as and if provided by the OIDC provider

8. Under the **Advanced** section, under **Claims Mapping**, enter the required field information to map the claim keys against the AppViewX User Label for the user profile information to be stored in the AppViewX expected format.

Advanced

Local authorization
☐

API Key

Claims Mapping

User Label	Claim Name	Delimiter
* User Name	sub	
* First Name	given_name	
* Last Name	family_name	
* Email	email	
Phone number	phone_number	
User Groups		

Add

Save

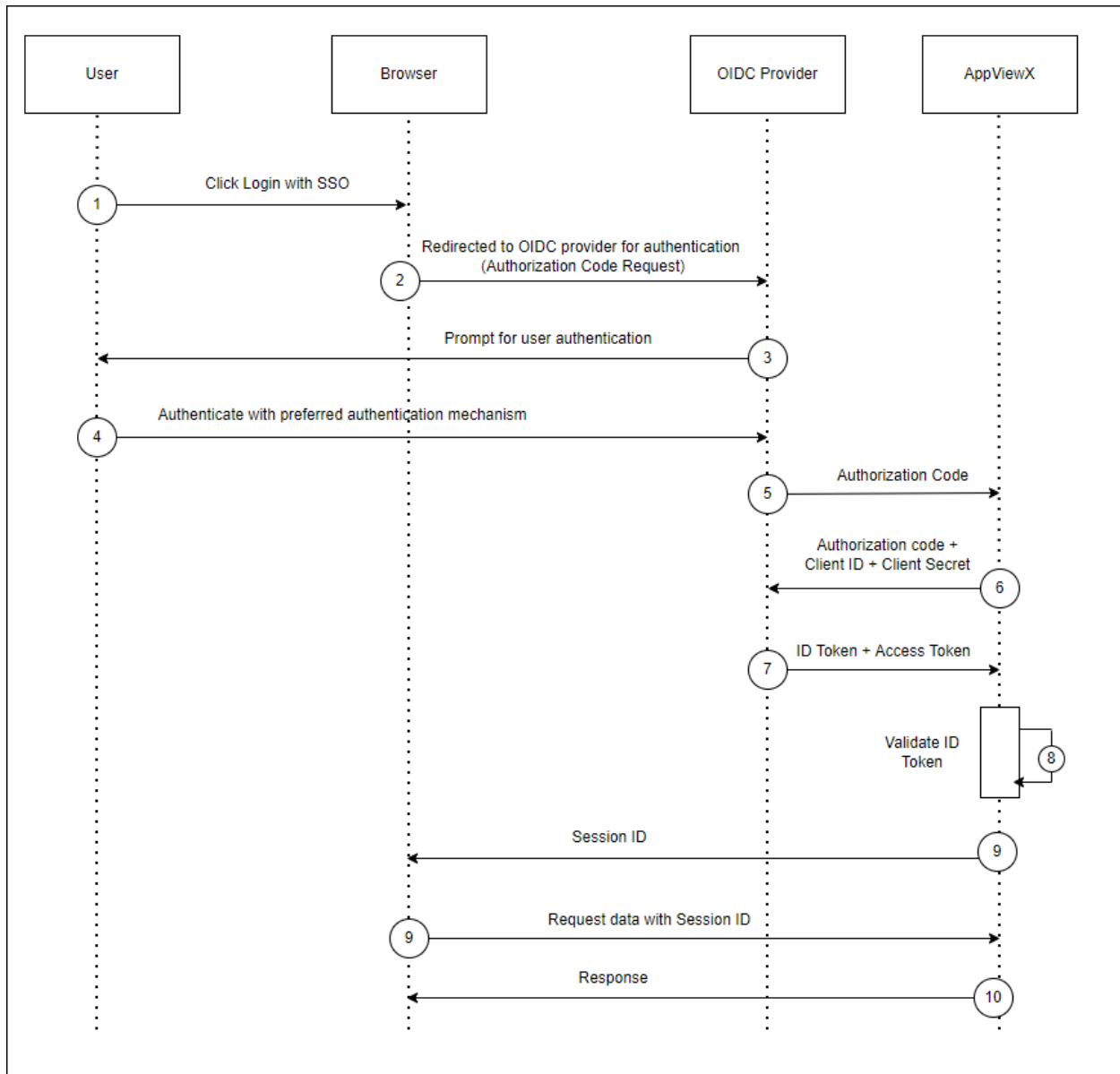
Cancel

Reset

For example:

- An identity provider can send the user login name with the key called sub in the ID token and another identity provider can send the user login name with the key called upn.
- The administrator can configure/modify the claim setting against the User Name either as sub or upn based on the ID claim response sent by the OIDC vendor.
- Similarly, custom claims can be configured and additional claims for the user profile if required. Currently, these custom claims stored in the user profile will not be shown along with the user profile on the AppViewX web application.

Login Workflow



1. When user tries to login with SSO in AppViewX, user will be redirected to the OIDC provider's login page.
2. The user can now use the preferred authentication mechanism to login to the OIDC. After successful authentication, OIDC provider will send Authorization code to AppViewX.
3. AppViewX will then send the Client ID and Client Secret along with that Authorization code to the OIDC provider.
4. OIDC provider validates the client credentials and authorization. On successful validation, it returns ID Token and Access Token to AppViewX.

5. AppViewX validates the ID token and uses the user information received in ID token.
6. If a user tries to login for the first time, then that user account will be created in AppViewX using the details fetched from ID Token.
7. If Local Authorization is enabled, then the admin has to map the user to the respective user group for providing the necessary permission and scope of management. Only then, the user can login to the AppViewX console. Until then the user will be getting an error while trying to login to AppViewX.
8. If Local Authorization is disabled, then the authorization in AppViewX will be performed based on the groups the user exists in IDP.
9. AppViewX will compare the user group details available in the ID token with the existing user groups in AppViewX. If the same user groups exists in both, then the user will be assigned with permissions and the scope of those groups. Else, user won't have any permissions within AppViewX.



Note: For Microsoft Azure, the token configuration should be configured with custom claims for sending user login name with the claim as upn and a group claim to send security groups as User Group.

Steps to Integrate OIDC

To integrate with AppViewX – Azure using OIDC

1. From the Microsoft Azure Home > Default Directory Overview page, create an app under Enterprise Application within the **Azure Active Directory** (AAD). Click **Enterprise applications**.

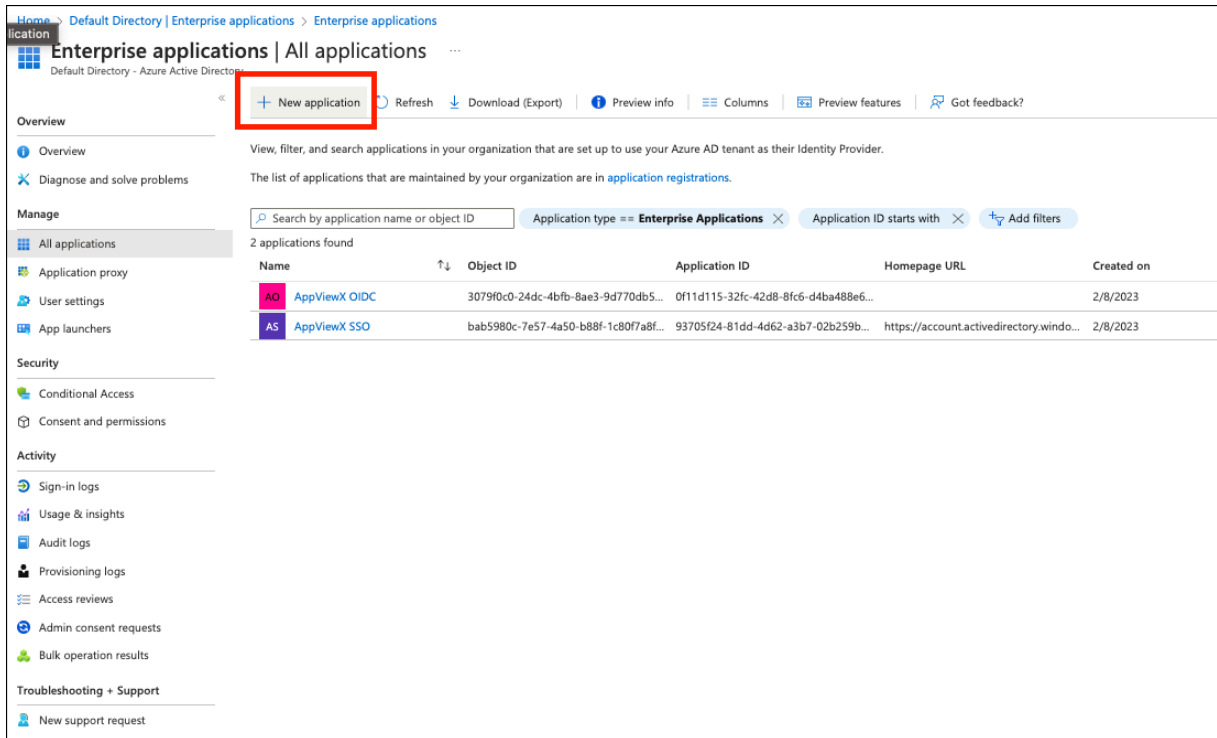
The screenshot shows the Microsoft Azure Default Directory Overview page. The left navigation pane includes links for Overview, Preview features, Diagnose and solve problems, and Manage. Under the Manage section, 'Enterprise applications' is highlighted with a red box. The main content area displays basic information for the Default Directory, including its name, tenant ID, primary domain, and license. There are also alerts for upcoming Authenticator number matching enforcement, IPv6 support, and MFA Server deprecation.

Basic information	
Name	Default Directory
Tenant ID	271bd2a5-5980-42b7-bcc2-f9cdc943701f
Primary domain	mallayaganesh3gmail.onmicrosoft.com
License	Azure AD Free

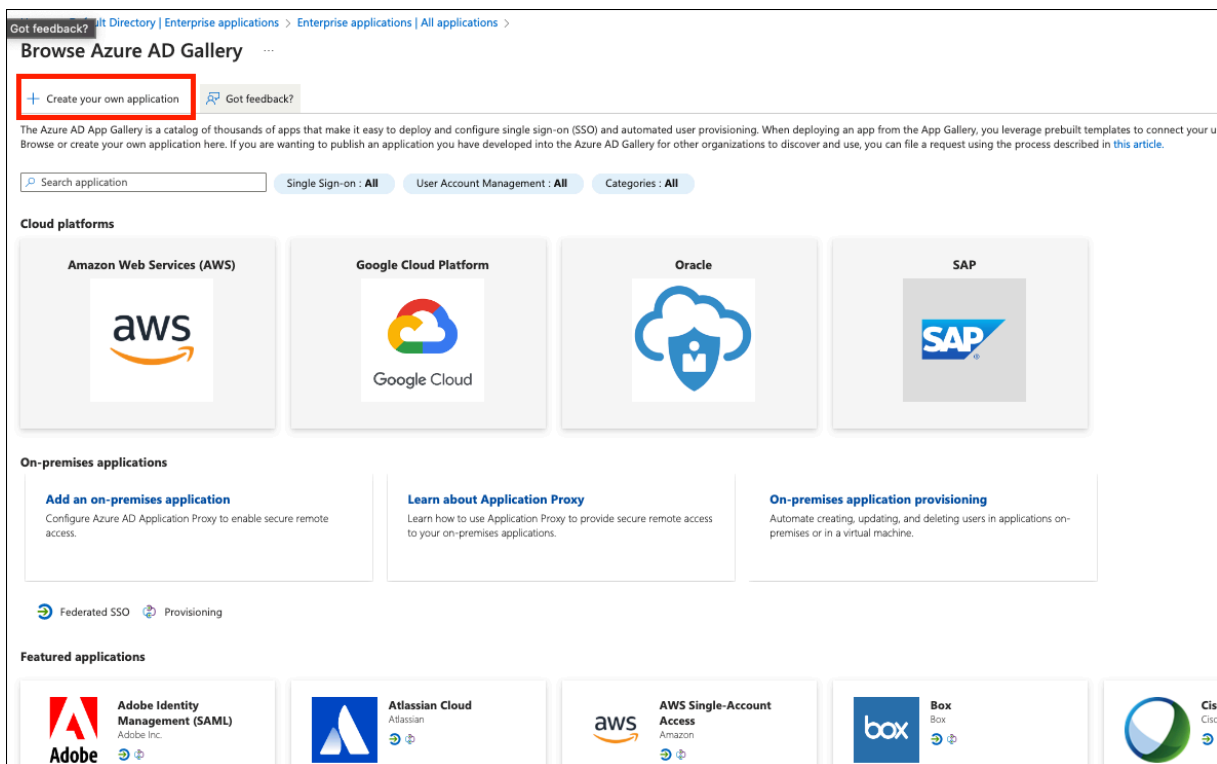
Alerts	
Upcoming Authenticator number matching enforcement Microsoft Authenticator number matching admin controls will be removed after February 27, 2023. Number matching will be enforced for all Microsoft Authenticator users after this date. Learn more	Upcoming IPv6 support in Azure AD Please review the upcoming IPv6 support and the steps required by March 31st to prevent any potential blocking of user sign-ins. Learn more
Upcoming MFA Server deprecation Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid any service impact. Learn more	

My feed	
Try Microsoft Entra admin center Secure your identity environment with Azure AD, permissions management and more. Go to Microsoft Entra	Ganesh Mallaya c646c3de-01cf-4ea8-87ae-15e18c601e2b Global Administrator View role information View profile
Azure AD Connect Not enabled Sync has never run Go to Azure AD Connect	

2. Click **New application**.



3. Click **Create your own application**.



4. In the Create your own application slider screen, perform the following:

Home > Default Directory > Enterprise applications > Enterprise applications > All applications >

Browse Azure AD Gallery

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you can use the app's configuration to create your own application. If you are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request.

Search application | Single Sign-on: All | User Account Management: All | Categories: All

Cloud platforms

- Amazon Web Services (AWS)
- Google Cloud Platform
- Oracle

On-premises applications

- Add an on-premises application
- Learn about Application Proxy
- On-premises application proxy

Featured applications

- Adobe Identity Management (SAML)
- Atlassian Cloud
- AWS Single-Account Access
- box

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

AppViewX OIDC SSO Enter a Name Step 1

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application
☐ Register an application to integrate with Azure AD (App you're developing)
☒ Integrate any other application you don't find in the gallery (Non-gallery) Step 2

Step 3

Create

- Enter a name in the **What's the name of your app?** field
 - Select the radio button **Integrate any other application you don't find in the gallery**
 - Click **Create**
5. The application is created successfully and the details are displayed as shown below. Verify the details.

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery >

AppViewX OIDC SSO | 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

Audit logs

Provisioning logs

Access reviews

Troubleshooting + Support

Properties

Name

AppViewX OIDC SSO

Application ID

d23e412b-b329-41fb-9df...

Object ID

e9a3511b-41a8-4a55-b4...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

2. Set up single sign on

Enable users to sign into their application using their Azure AD credentials

[Get started](#)

3. Provision User Accounts

Automatically create and delete user accounts in the application

[Get started](#)

4. Conditional Access

Secure access to this application with a customizable access policy.

[Create a policy](#)

5. Self service

Enable users to request access to the application using their Azure AD credentials

[Get started](#)

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

Application Created.

6. Navigate to AAD Overview and click **App Registration**.

Home >

Default Directory | Overview

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Custom security attributes (Preview)

Licenses

Cross-tenant synchronization (Preview)

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

+ Add

Manage tenants

What's new

Preview features

Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. [Try the new Microsoft Entra admin center!](#)

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	Default Directory	Users	2
Tenant ID	271bd2a5-5980-42b7-bcc2-f9cdc943701f	Groups	1
Primary domain	mallayaganesh3gmail.onmicrosoft.com	Applications	3
License	Azure AD Free	Devices	0

Alerts

Upcoming Authenticator number matching enforcement

Microsoft Authenticator number matching admin controls will be removed after February 27, 2023. Number matching will be enforced for all Microsoft Authenticator users after this date.

[Learn more](#)

Upcoming IPv6 support in Azure AD

Please review the upcoming IPv6 support and the steps required by March 31st to prevent any potential blocking of user sign-ins.

[Learn more](#)

Upcoming MFA Server deprecation

Please migrate from MFA Server to Azure Factor Authentication by September 20, any service impact.

[Learn more](#)

My feed

Try Microsoft Entra admin center

Secure your identity environment with Azure AD.

Ganesh Mallaya

c646c3de-01cf-4ea8-87ae-15e18c601e2b

Azure AD Connect

Not enabled

7. Select the App created in step 4.

The screenshot shows the 'Default Directory | App registrations' page in the Azure portal. A red arrow points to the 'AppViewX OIDC SSO' application in the list. The table below shows the details of the applications found.

Display name	Application (client) ID	Created on	Certificates & secrets
AppViewX OIDC	0f11d115-32fc-42d8-8fc6-d4ba488e6a8e	2/8/2023	Current
AppViewX OIDC SSO	d23e412b-b329-41fb-9df3-2fc49213d8bf	2/9/2023	-
AppViewX SSO	93705f24-81dd-4d62-a3b7-02b259b8892c	2/8/2023	-

8. Setup the Redirect URI for web-based application. Click **Redirect URI** from the overview page of the App.

The screenshot shows the 'AppViewX OIDC SSO' app overview page. The 'Redirect URI' link is highlighted with a red box. The page displays the following information:

- Display name: AppViewX OIDC SSO
- Application (client) ID: d23e412b-b329-41fb-9df3-2fc49213d8bf
- Object ID: 142fd8b7-0e20-4d87-a55c-36eb33450623
- Directory (tenant) ID: 271bd2a5-5980-42b7-bcc2-f9cd943701f1
- Supported account types: My organization only
- Client credentials: Add a certificate or secret
- Redirect URIs: Add a Redirect URI
- Application ID URI: Add an Application ID URI
- Managed application in: AppViewX OIDC SSO

The page also includes a 'Get Started' section with a 'Build your application with the Microsoft identity platform' banner and three quickstart guides: 'Call APIs', 'Sign in users in 5 minutes', and 'Configure for your organization'.

9. Click **Add a Platform**.

The screenshot shows the 'AppViewX OIDC SSO | Authentication' configuration page. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled 'Platform configurations' and includes a note about implicit grant and logout URI settings. A red box highlights the '+ Add a platform' button. Below this, there are sections for 'Front-channel logout URL', 'Implicit grant and hybrid flows' (with 'ID tokens' selected), and 'Supported account types' (with 'Accounts in this organizational directory only' selected).

Home > Default Directory | App registrations > AppViewX OIDC SSO

AppViewX OIDC SSO | Authentication

Search < Got feedback?

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

To configure single sign-on, including SAML-based sign-on, try [Enterprise applications](#).

+ Add a platform

NOTE: You have implicit grant and/or logout URI settings set without any Web or SPA redirect URIs registered. You should remove these settings or register the appropriate redirect URI.

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://example.com/logout>

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

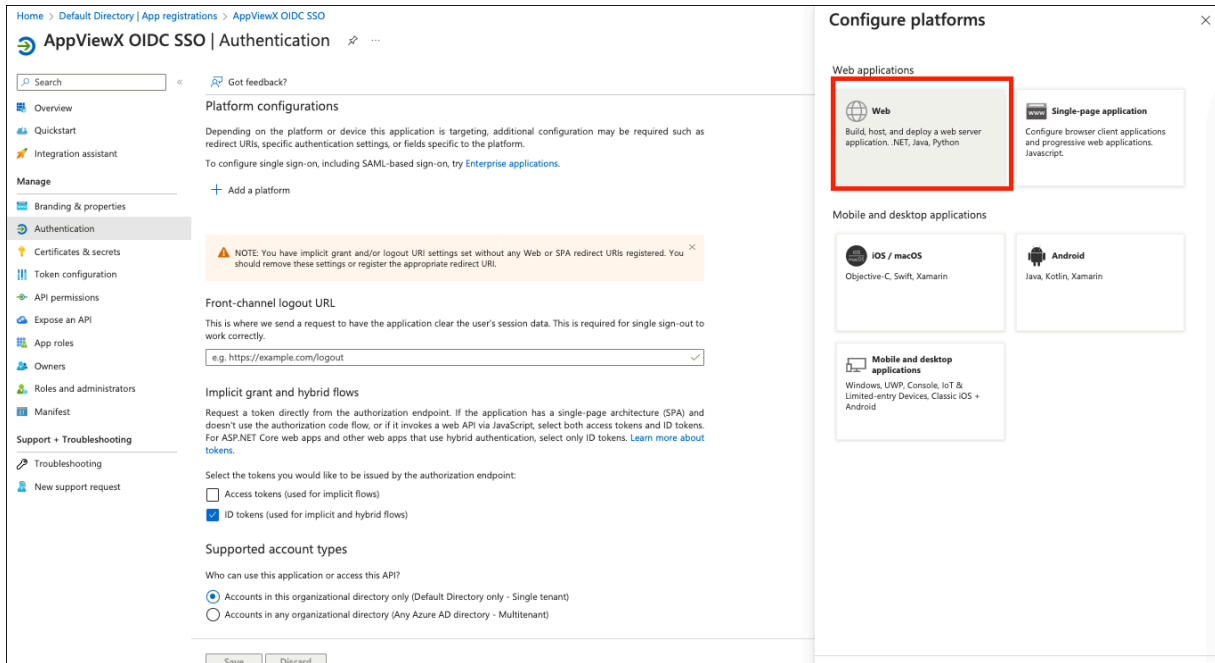
- ☐ Access tokens (used for implicit flows)
- ☒ ID tokens (used for implicit and hybrid flows)

Supported account types

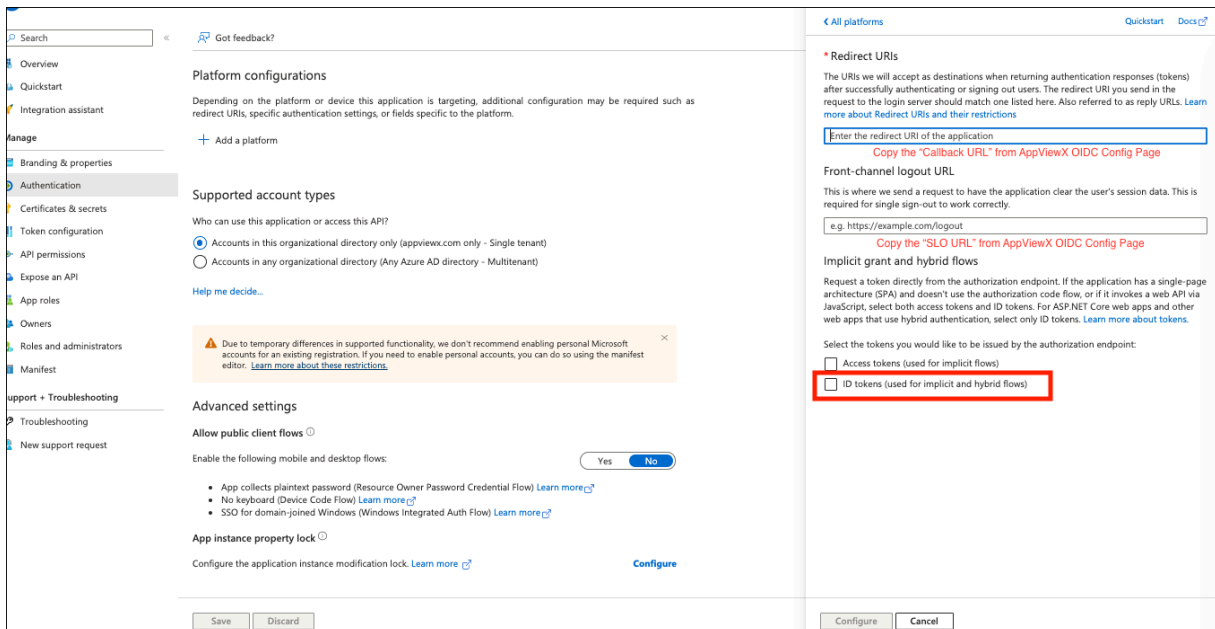
Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

10. Select the **Web** platform and copy-paste the links from the AppViewX GUI.



11. Copy paste the URL from AppViewX GUI as follows:



- Copy the Callback URL from AppViewX GUI to the first field on the right
- Copy the SLO URL from AppViewX GUI to the second field on the right
- Select the check box **ID Tokens (used for implicit and hybrid flows)**

d. Click **Configure**

Enable SSO ☒

* Authentication Protocol ☐ SAML ☒ OIDC

Service Provider Information

Data center: cloud-dc

* Appviewx Host: <https://appdemo-gm.appvx.com>

Callback URL: <https://appdemo-gm.appvx.com/appviewx/oidclogin>

SLO URL: <https://appdemo-gm.appvx.com/appviewx/logout?oidcLogout=true>

① Register AppViewX as a client in OIDC provider with the Callback URL and Logout URL, then configure this setting with Client details.

IDP Configuration

12. Verify the details of the Redirect URI.

AppViewX SE Demo App | Authentication

Search Got feedback?

Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

<https://appdemo-gm.appvx.com/appviewx/oidclogin> ← **Callback URL**

[Add URI](#)

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

<https://appdemo-gm.appvx.com/appviewx/logout?oidcLogout=true> ← **SLO URL**

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows) ←

13. Click **Token configuration** which will help setup the Group and User Claim settings.

Home > appviewx.com | App registrations > AppViewX SE Demo App

Search < Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets**
 - Token configuration**
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Essentials

Display name : AppViewX SE Demo App

Application (client) ID : 1ed4483b-ae38-48d9-99ae-846d9a87aeb7

Object ID : 08ef436e-7ba8-462b-b829-502a270d5480

Directory (tenant) ID : b3ac14d4-f14b-490d-a1c9-c9e9546285be

Supported account types : My organization only

Client credentials : 0 certificate, 3 secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in I... : AppViewX SE Demo App

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 for existing applications. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

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.

[View API permissions](#)

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.

[View all quickstart guides](#)

Configure for your organization

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

[Go to Enterprise applications](#)

14. In the Token configuration screen, click **Add optional claim**.

Home > appviewx.com | App registrations > AppViewX SE Demo App

Search < Got feedback?

AppViewX SE Demo App | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

[+ Add optional claim](#) [+ Add groups claim](#)

Claim ↑↓	Description
No results.	

Perform the following on the right slider screen:

Configuring Authentication Settings

Home > appviewx.com | App registrations > AppViewX SE Demo App

AppViewX SE Demo App | Token configuration

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑

Description

No results.

Add optional claim

Cancel

* Token type

Access and ID tokens are used by applications for authentication. [Learn more](#)

☒ ID

☐ Access

☐ SAML

Claim ↑

Description

☐ cty	User's country/region
☒ email	The addressable email for this user, if the user has one
☒ family_name	Provides the last name, surname, or family name of the us...
☐ fhd	IP address
☒ given_name	Provides the first or "given" name of the user, as set on th...
☐ in_corp	Signals if the client is logging in from the corporate netw...
☐ ipaddr	The IP address the client logged in from
☐ login_hint	Login hint
☐ onprem_sid	On-premises security identifier
☐ preferred_username	Provides the preferred username claim, making it easier f...
☐ pwd_exp	The datetime at which the password expires
☐ pwd_url	A URL that the user can visit to change their password
☐ sid	Session ID, used for per-session user sign out
☐ tenant_ctry	Resource tenant's country/region
☐ tenant_region_scope	Region of the resource tenant
☒ upn	An identifier for the user that can be used with the userna...
☐ verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail

Add Cancel

a. In the Token type, select the **ID** radio button

b. Select the following claims below

c. Click **Add**

Now click **Add group claims** and perform the following on the right slider screen.

Home > appviewx.com | App registrations > AppViewX SE Demo App

AppViewX SE Demo App | Token configuration

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑

Description

Token type ↑

Optional settings

email	The addressable email for this user, if the user has one	ID	-
family_name	Provides the last name, surname, or family name of the user as defined in the user object	ID	-
given_name	Provides the first or "given" name of the user, as set on the user object	ID	-
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and should not b...	ID	Default

a. Select the **Security groups** checkbox

b. From the ID section select the radio button for **sAMAccountName**

15. Copy paste the Claims Mapping from Columns Claim in AppViewX as below.

Advanced

Local authorization

☐

API Key

Claims Mapping

User Label	Claim Name	Delimiter
* User Name	upn	
* First Name	given_name	
* Last Name	family_name	
* Email	email	
Phone number	phone_number	
User Groups	groups	

Add

16. To create API permissions for claim mapping, click **API Permissions**.

Home > appviewx.com | App registrations >

AppViewX SE Demo App

Search

Directory (tenant) ID

Delete

Endpoints

Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Essentials

Display name

: AppViewX SE Demo App

Application (client) ID

: 1ed4483b-ae38-48d9-99ae-846d9a87aeb7

Object ID

: 08ef436e-7ba8-462b-b829-502a270d5480

Directory (tenant) ID

: b3ac14d4-ff4b-490d-a1c9-c9e9546285be

Supported account types

: My organization only

Client credentials

: 0 certificate, 3 secret

Redirect URIs

: 1 web, 0 spa, 0 public client

Application ID URI

: Add an Application ID URI

Managed application in I...

: AppViewX SE Demo App

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 not add new features. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started

Documentation

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.

View API permissions

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.

View all quickstart guides

Configure for your organization

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

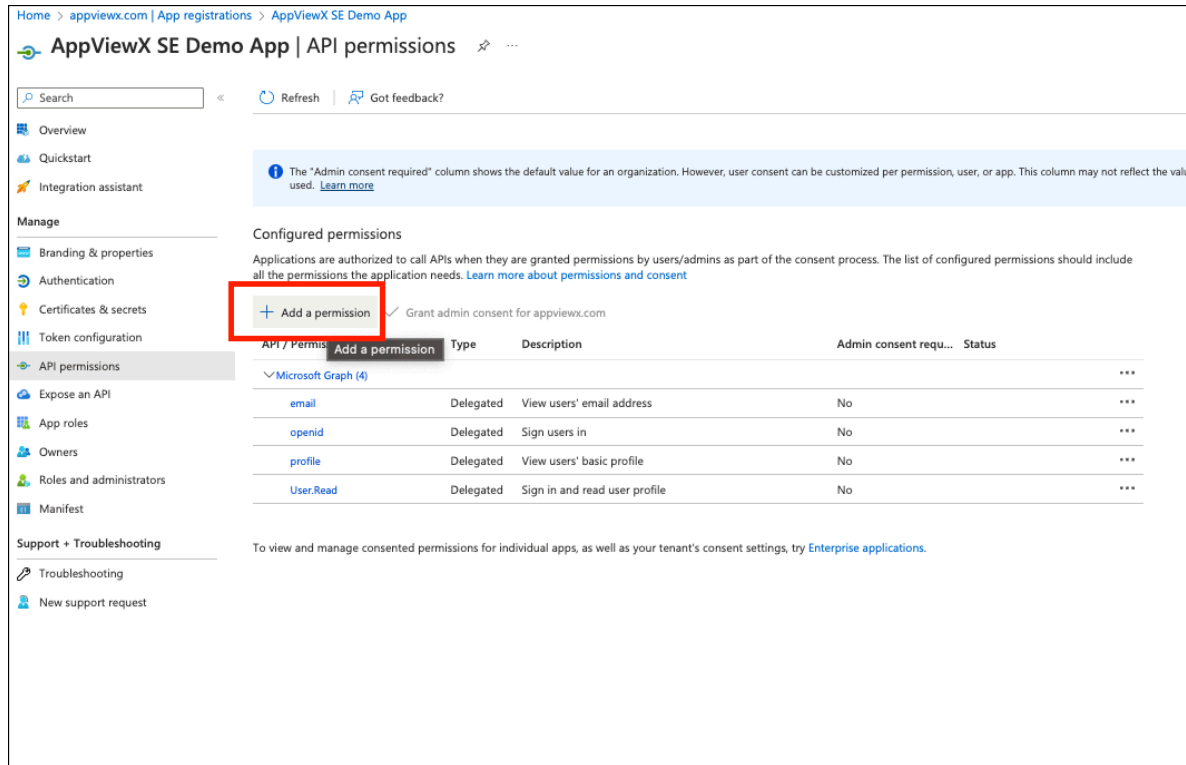
Go to Enterprise applications

17. To configure the API Permissions from Microsoft Graph.

Copyright © 2023 [AppViewX, Inc]. All Rights Reserved.

99

a. Click **Add a Permissions**.



Home > appviewx.com | App registrations > AppViewX SE Demo App

AppViewX SE Demo App | API permissions

Search Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value used. [Learn more](#)

Configured permissions

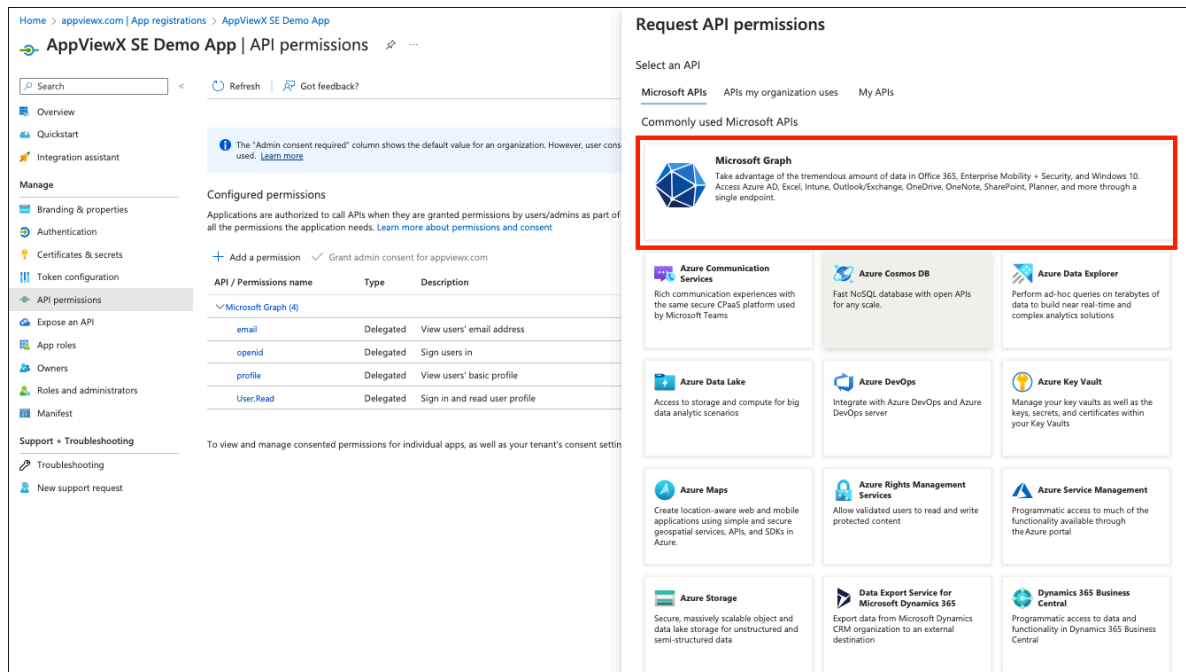
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for appviewx.com

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (4)				...
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

b. Select **Microsoft Graph**



Home > appviewx.com | App registrations > AppViewX SE Demo App

AppViewX SE Demo App | API permissions

Search Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for appviewx.com

API / Permissions name	Type	Description
Microsoft Graph (4)		
email	Delegated	View users' email address
openid	Delegated	Sign users in
profile	Delegated	View users' basic profile
User.Read	Delegated	Sign in and read user profile

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Cosmos DB

Fast NoSQL database with open APIs for any scale

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Maps

Create location-aware web and mobile applications using simple and secure geospatial services, APIs, and SDKs in Azure.

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

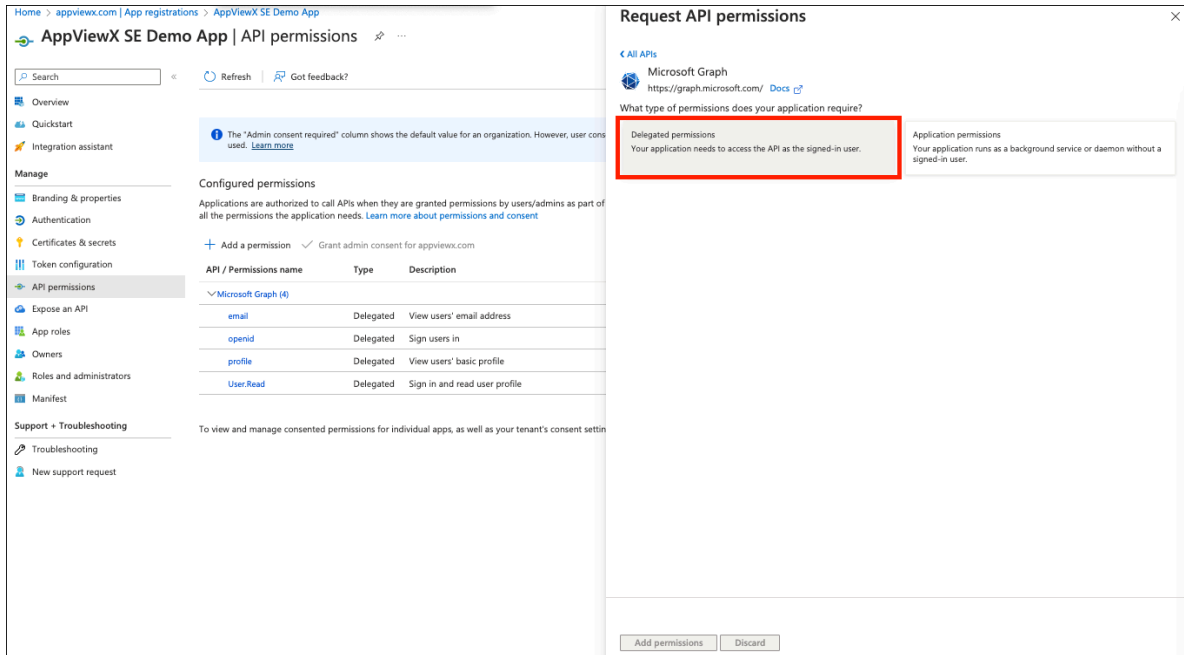
Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central

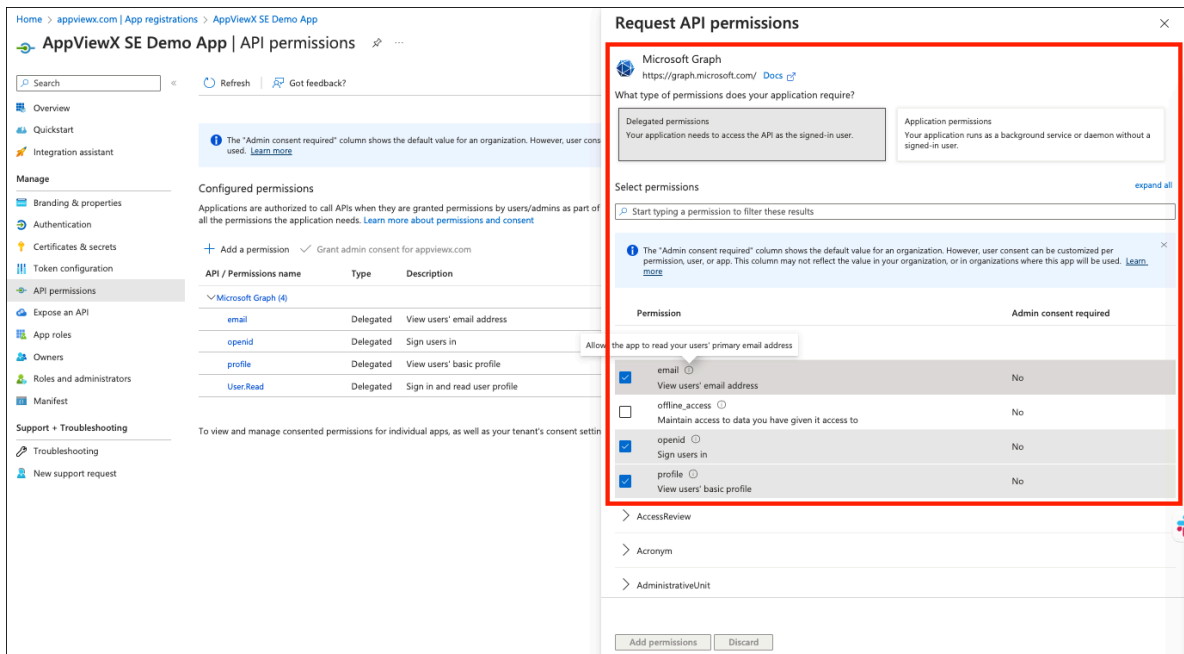
Programmatic access to data and functionality in Dynamics 365 Business Central

c. Select **Delegated permission**

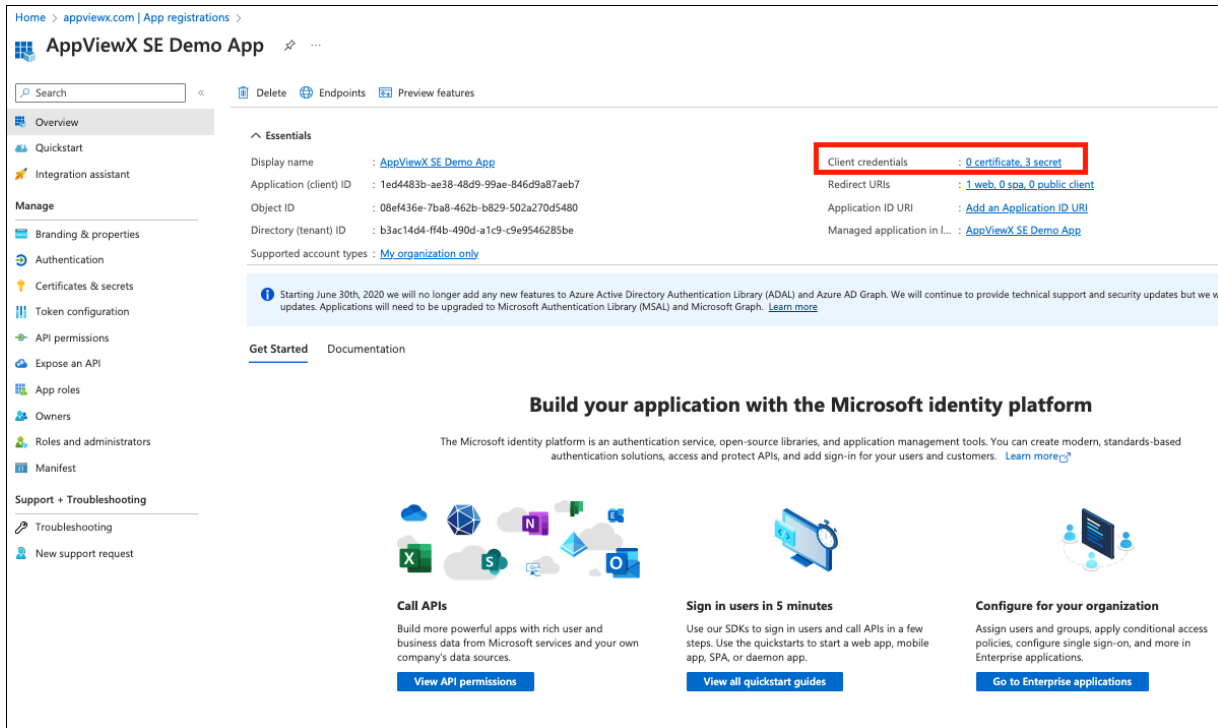


d. Click the following check-box on the Select Permissions section

- email
- openid
- profile



18. To create client secret for the App, click **Client credentials**.



Home > appviewx.com | App registrations > AppViewX SE Demo App

Search < Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest

Support + Troubleshooting Troubleshooting New support request

Essentials

Display name : AppViewX SE Demo App

Application (client) ID : 1ed4483b-ae38-48d9-99ae-846d9a87aeb7

Object ID : 08e436e-7ba8-462b-b829-502a270d5480

Directory (tenant) ID : b3ac14d4-ff4b-490d-a1c9-c9e9546285be

Supported account types : My organization only

Client credentials : 0 certificate, 3 secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in L... : AppViewX SE Demo App

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 not add new features. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Build your application with the Microsoft identity platform

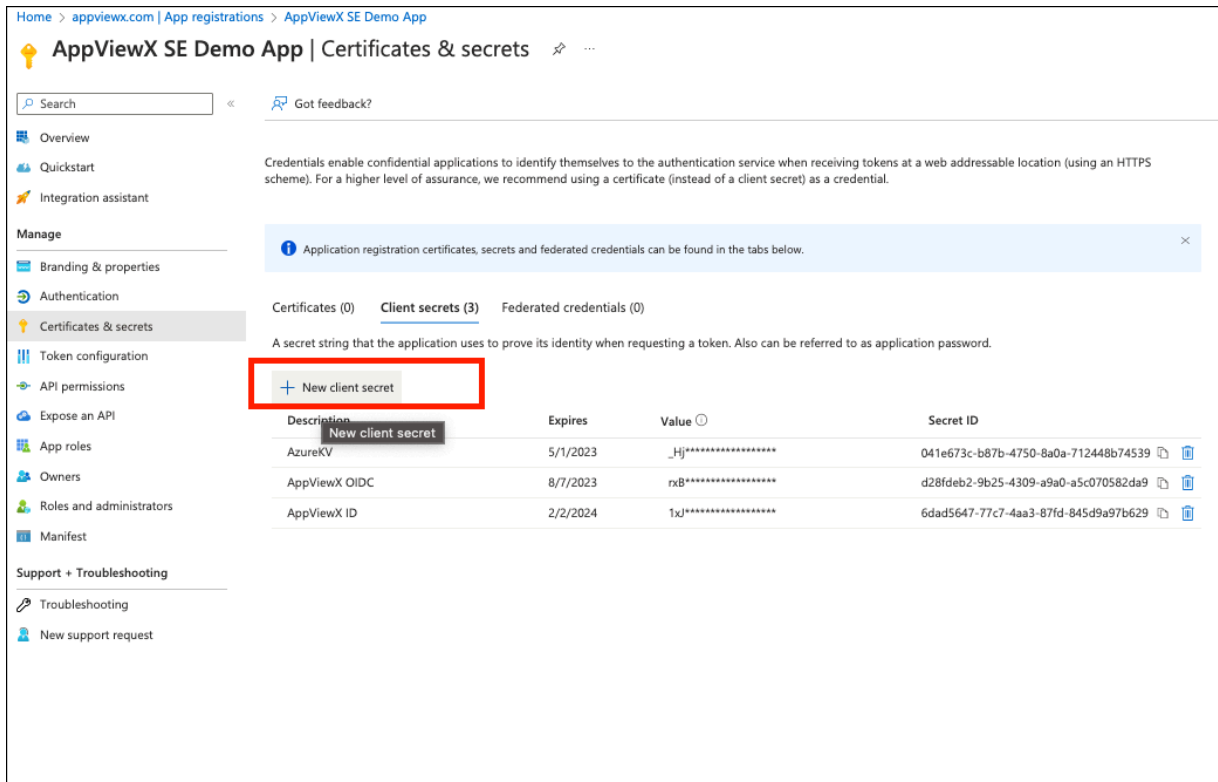
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Call APIs Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. [View API permissions](#)

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. [View all quickstart guides](#)

Configure for your organization Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications. [Go to Enterprise applications](#)

- Click **New client secret**, copy the secret and save it securely.



Home > appviewx.com | App registrations > AppViewX SE Demo App

AppViewX SE Demo App | Certificates & secrets

Search < Got feedback?

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest

Support + Troubleshooting Troubleshooting New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

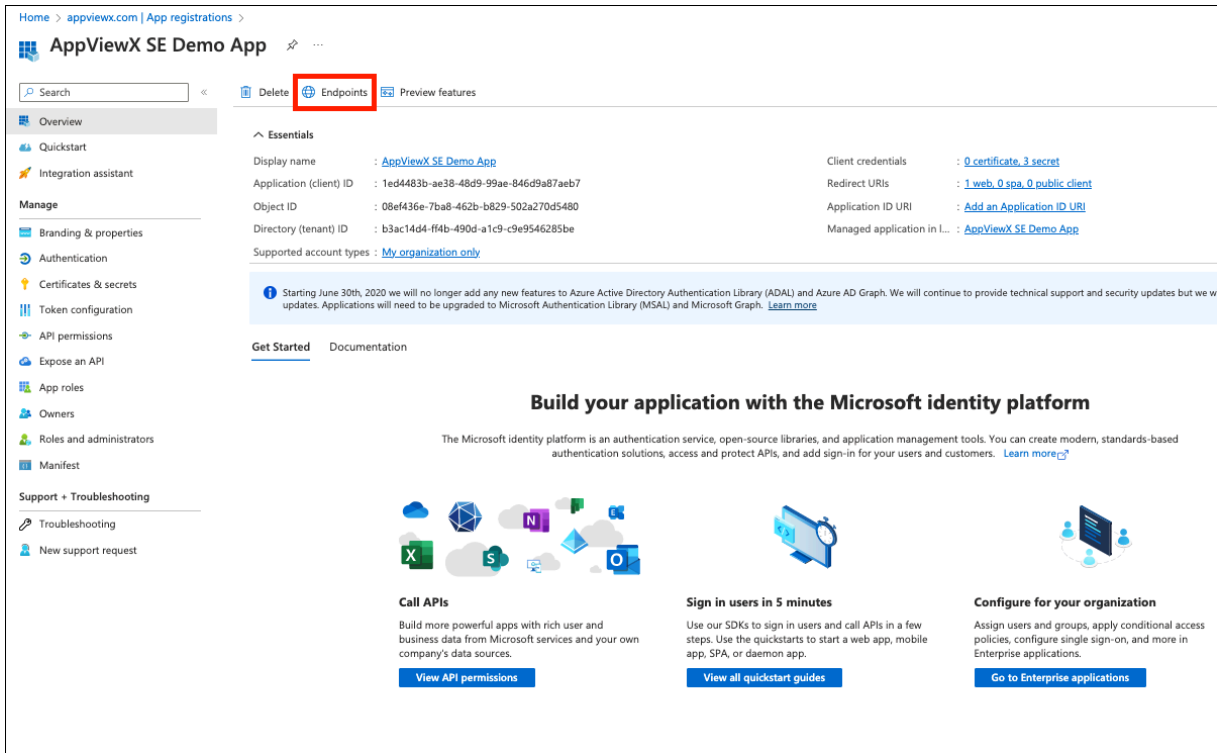
Certificates (0) Client secrets (3) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

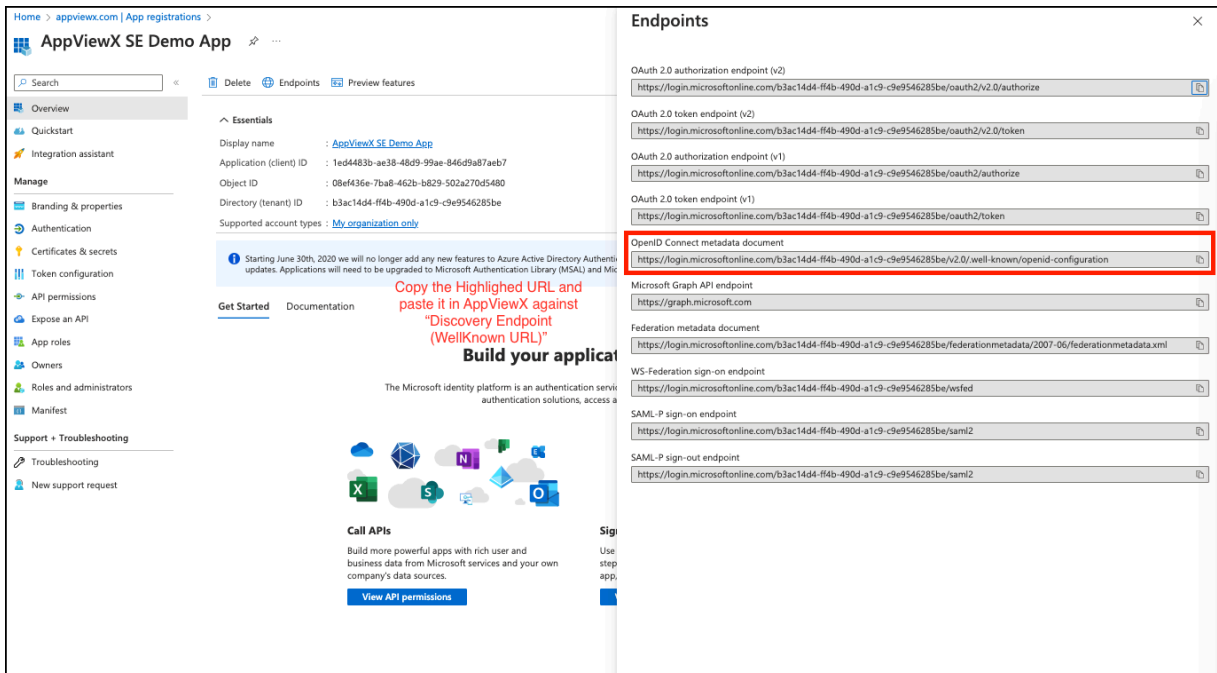
+ New client secret

Description	Expires	Value	Secret ID
New client secret	5/1/2023	_Hj*****	041e673c-b87b-4750-8a0a-712448b74539
AppViewX OIDC	8/7/2023	rxB*****	d28fdeb2-9b25-4309-a9a0-a5c070582da9
AppViewX ID	2/2/2024	1xj*****	6dad5647-77c7-4aa3-87fd-845d9a97b629

19. To copy the Endpoint Details from App Overview Page, click **Endpoints**.



- Copy the highlighted URL and paste it in AppViewX against **Discovery Endpoint (WellKnown URL)**.



20. Configure the Client ID, Secret Key and OpenID Wellknown URL in AppViewX GUI.

IDP Configuration

*

Client Name

AppViewX OIDC

?

*

Client ID

1ed4483b-ae38-48d9-99ae-846d9a87aeb7

?

*

Client Secret

.....

?

*

Discovery Endpoint
(WellKnown URL)

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/

Fetch details

?

✔ Required OIDC provider details are fetched successfully. [View details.](#)

Advanced

Register

IDP Configuration

OIDC Provider details

Issuer

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/v2.0

?

Authorization EndPoint

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/oauth2/v2.0/authorize

?

Token End Point

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/oauth2/v2.0/token

?

Public Key URI

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/discovery/v2.0/keys

?

End Session Endpoint

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/oauth2/v2.0/logout

?

*

Discovery Endpoint
(WellKnown URL)

https://login.microsoftonline.com/b3ac14d4-ff4b-490d-a1c9-c9e9546285be/

Fetch details

?

✔ Required OIDC provider details are fetched successfully. [View details.](#)

Advanced

21. Create the Security Group from Azure in AppViewX (add this in the Accounts >> User groups) and then try user authentication. Ensure that the AppViewX roles are mapped to the user groups.



Note: Use the Security groups with Source as **Windows Server AD**

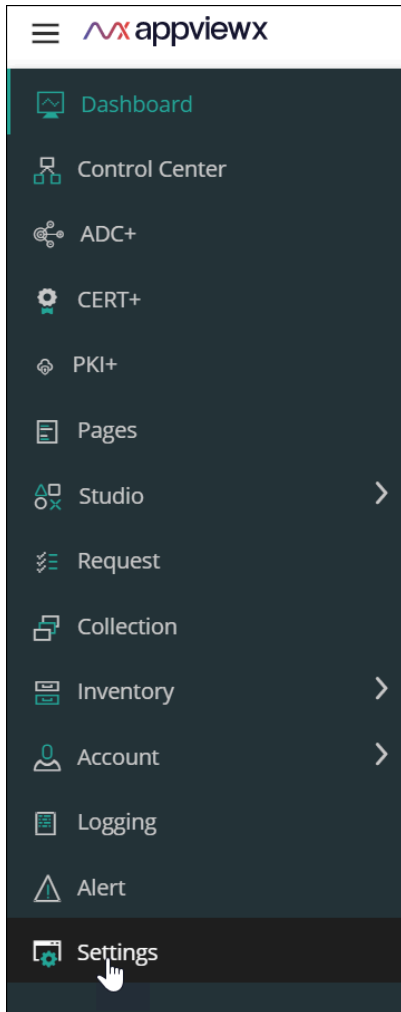
Group type	Membership type	Email	Source
Security	Assigned		Windows Server AD
Security	Assigned		Cloud
Security	Assigned		Cloud
Security	Assigned		Windows Server AD
Security	Assigned		Windows Server AD
Security	Assigned		Cloud
Security	Assigned		Windows Server AD
Security	Assigned		Windows Server AD

Configuring the IP Restrictions

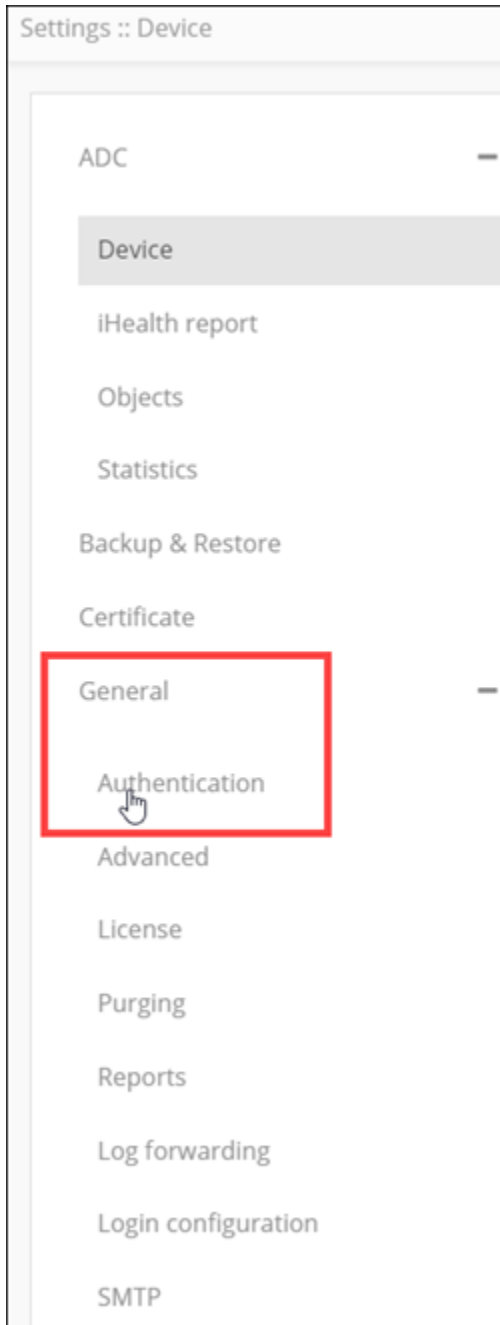
For enhanced security and if the administrator wants to whitelist specific IP addresses for user login, AppViewX lets you configure IP restrictions to allow access from whitelisted IP addresses/subnet ranges.

To configure IP restrictions:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

The screenshot shows the 'Settings :: Authentication' page with the 'General information' tab selected. The left sidebar lists various settings categories: ADC, Device, Health report, Objects, Statistics, Backup & Restore, Certificate, General, Authentication (selected), Advanced, License, Purging, Reports, Log forwarding, Login configuration, and SMTP. The main content area displays the following fields:

- Host:** Text input field.
- Port:** Text input field with the value '389'.
- LDAPS:** Toggle switch, currently turned off.
- Upload certificate:** Text input field with a 'Browse' button.
- Bind DN:** Text input field with the value 'CN=admin,DC=example,DC=com'.
- Bind password:** Text input field.
- Data center:** Dropdown menu with the value 'dc1'.
- Authorization:** Toggle switch, currently turned off.
- Enable Nested Groups:** Toggle switch, currently turned off.
- LDAP Sync:** Toggle switch, currently turned off.

5. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.

The screenshot shows the 'Settings :: Authentication' page with the 'IP Restriction' tab selected. The left sidebar is the same as the previous screenshot. The main content area displays the following fields:

- General information:**
 - Enable IP Restriction:** Toggle switch, currently turned off.
- IP/Subnet Configuration:**
 - Rule Name:** Text input field.
 - User group:** Dropdown menu with the value 'Select User Group(s)'.
 - Mapping type:** Radio buttons for 'IP Range' (selected) and 'Subnet'.
 - Start IP:** Text input field with the value '192.1.2.3'.
 - End IP:** Text input field with the value '192.1.2.3'.
 - Buttons:** 'Add' and 'Reset' buttons.

6. In the **General Information** section, turn on the **Enable IP Restriction** toggle.

7. In the **IP/Subnet Configuration** section, enter the required field information.

IP/Subnet Configuration

*

Rule Name

Test_Rule

*

User group

admin usergroup

Mapping type

☐ IP Range
 ☒ Subnet

*

Subnet

192.1.2.3/4

Add

Reset

The following table describes the field information in this section:

Field	Description
*Rule Name	Rule name for a whitelisting condition.
*User group	Select the user group to which this rule will apply, from the dropdown menu, .  Note: Only the users from the selected user group will be allowed to login to AppViewX from the whitelisted IP address/subnet range.
Mapping Type	Select one of the two mapping types: • IP Range • Subnet
*Start IP	Enter the starting IP address for the whitelisted IP/subnet range.  Note: The IP/subnet range should be specified in the ascending order.  Note: This field is displayed only when Mapping Type is selected as IP Range.
End IP	Enter the ending IP address for the whitelisted IP/subnet range.  Note: The IP/subnet range should be specified in the ascending order.

Field	Description
	 Note: This field is displayed only when Mapping Type is selected as IP Range .
*Subnet	Enter the Subnet network range to whitelist.  Note: This field is displayed only when Mapping Type is selected as Subnet .

8. To save the IP restriction settings, click **Add** or to reconfigure the settings, click **Reset**.

The IP restriction settings thus configured are saved and displayed in the table shown at the end of the screen.

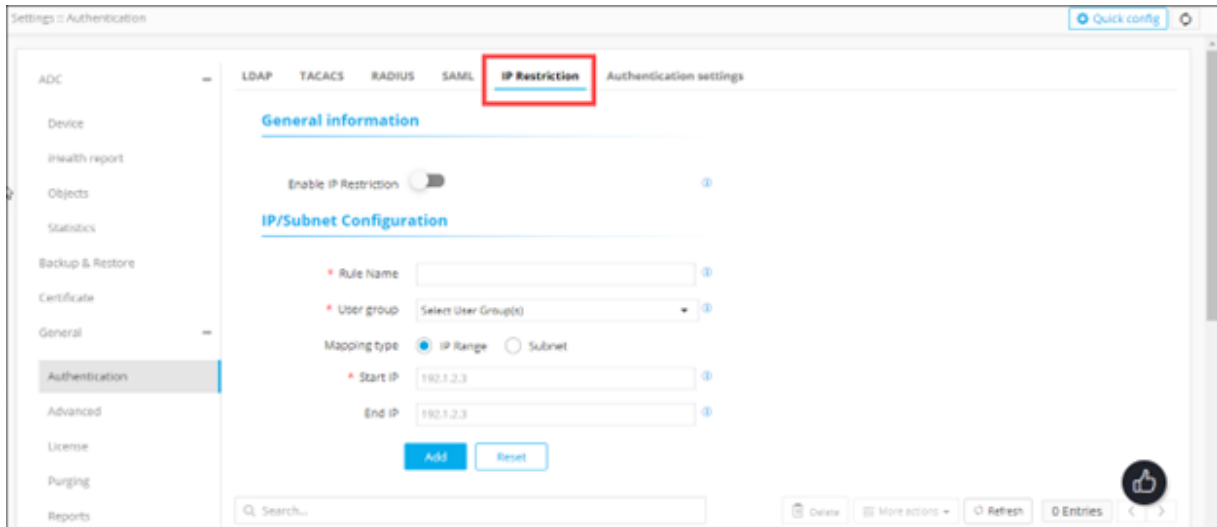
☐	Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
☐	test	admin usergroup	subnet	192.168.132.1/24			✔ Enabled
☐	Test_Rule	admin usergroup	subnet	192.1.2.3/4			✔ Enabled

- [Enabling a IP Restriction Rule](#)
- [Disabling an IP Restriction Rule](#)
- [Deleting an IP Restriction Rule](#)

Enabling a IP Restriction Rule

To enable a IP restrictions rule:

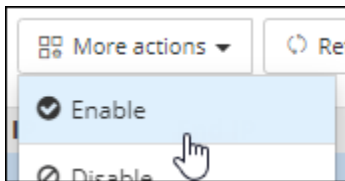
1. Navigate to the **Settings :: Authentication** page.
2. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.



- From the table at the end of the page, for the IP restrictions rule you want to enable, select the check box corresponding to that rule.

☒	Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
☒	Test_Rule	admin usergroup	subnet	192.1.2.3/4			Disabled

- From the **More actions** drop-down menu, click **Enable**.

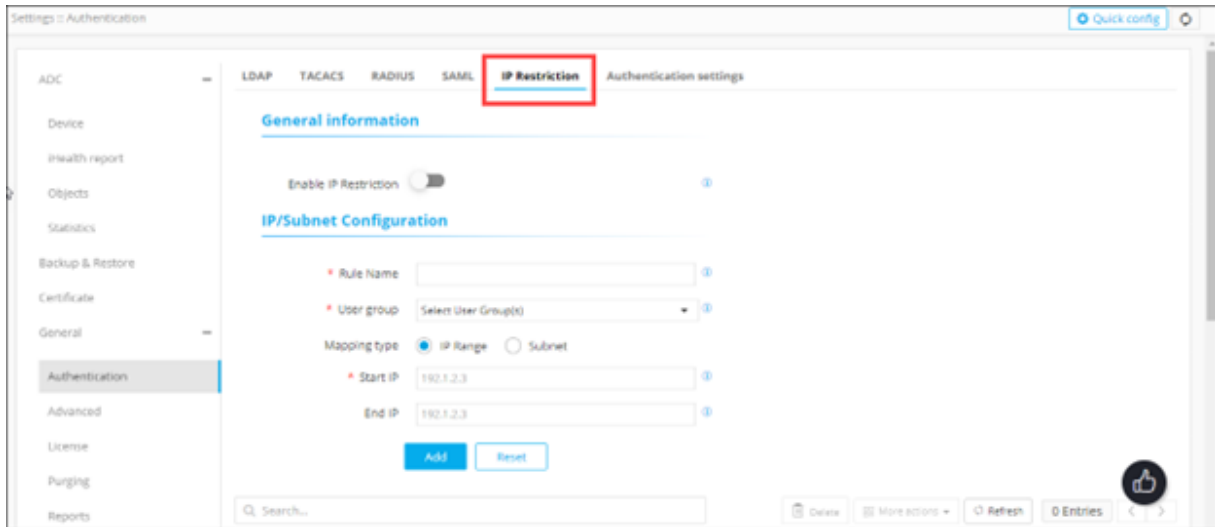


- In the **Enable** dialog box, click **Yes**.

Disabling an IP Restriction Rule

To disable a IP restrictions rule:

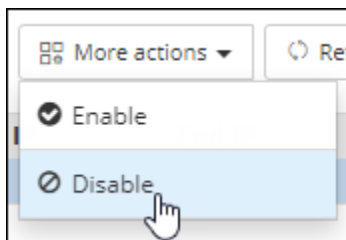
- Navigate to the **Settings :: Authentication** page.
- To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.



3. From the table at the end of the page, for the IP restrictions rule you want to disable, select the check box corresponding to that rule.

☒	Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
☒	Test_Rule	admin usergroup	subnet	192.1.2.3/4			Enabled

4. From the **More actions** drop-down menu, click **Disable**.

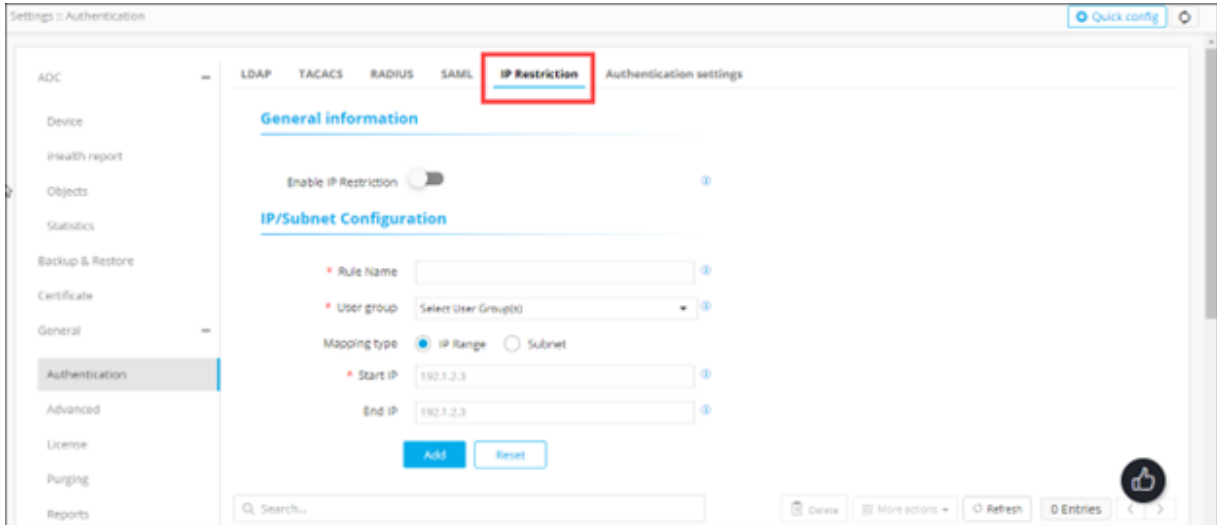


5. In the **Disable** dialog box, click **Yes**.
The selected rule is disabled.

Deleting an IP Restriction Rule

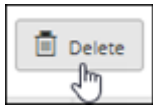
To delete an IP restrictions rule:

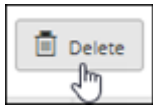
1. Navigate to the **Settings :: Authentication** page.
2. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.



- From the table at the end of the page, for the IP restrictions rule you want to delete, select the check box corresponding to that rule.

☒	Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
☒	Test_Rule	admin usergroup	subnet	192.1.2.3/4			Enabled



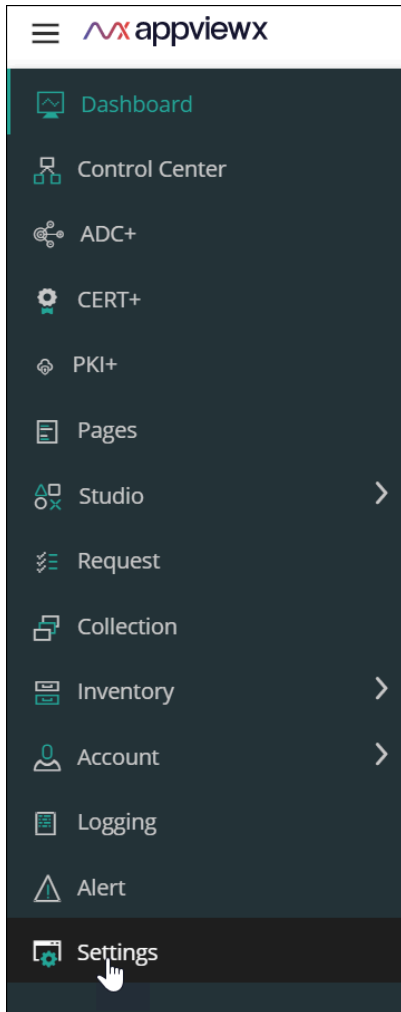
- Click .
- In the **Confirmation** dialog box, click **Yes**.
The selected rule is deleted.

Configuring Authentication Settings

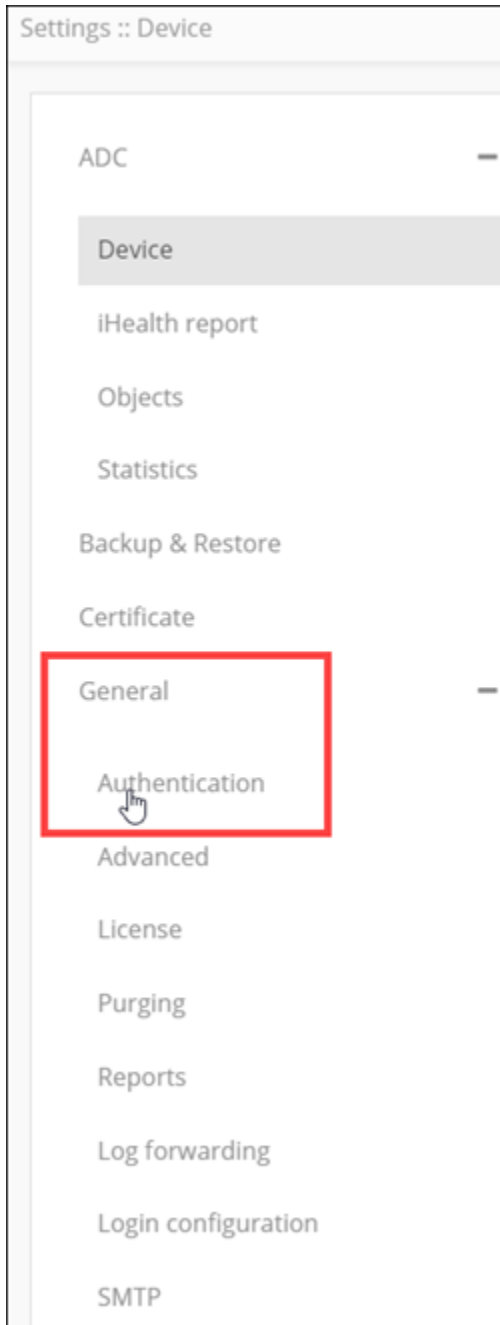
In addition to configuring authentication settings, AppViewX also lets you enable birthright provisioning for new users, configure the order in which user credentials are authenticated, enable/disable an authentication check, and other user and node settings.

To configure the authentication settings:

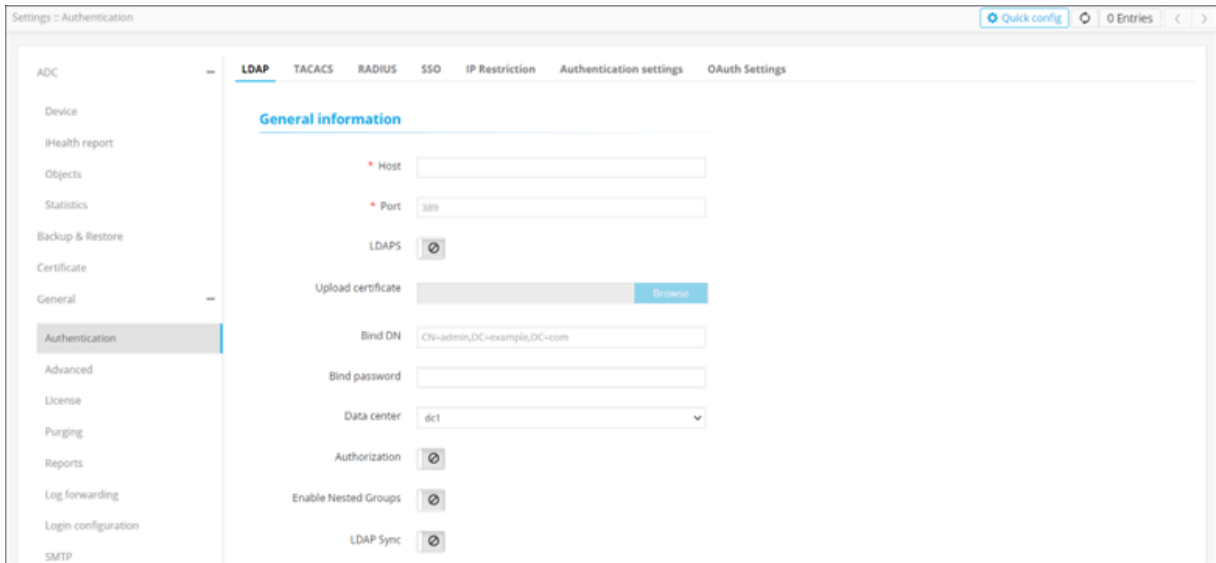
- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Settings**.



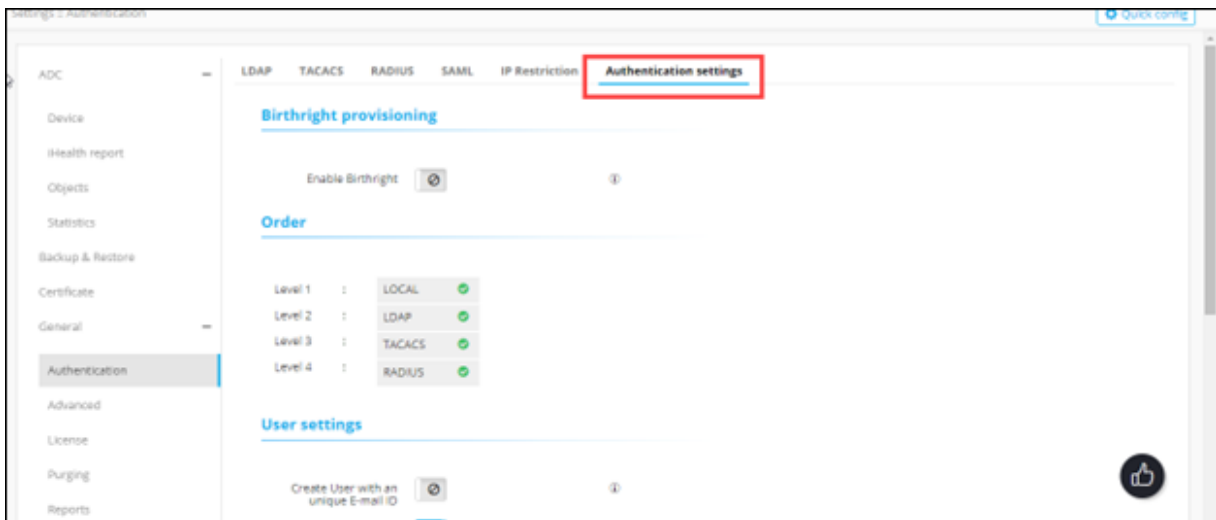
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. On the **Settings :: Authentication** page, click the **Authentication settings** tab.



6. To enable **BIRTHRIGHT provisioning** for new users who log into the system with a predefined set of permissions (associated with the user group), turn on the **Enable Birthright** toggle.
To do this, the admin should select the user group (Assigned with the defined permissions), which will act as a default user group for all the users logging in to AppViewX. For more details, refer to the content on creating a role and associating it with a user group.
7. To define the order in which the authentication settings will be checked, in the **Order** section, drag and drop the authentication labels to the required corresponding levels.
If the level 1 check is set to Local and the level 2 check is set to LDAP, user credentials will be authenticated locally first and then on the LDAP server.



Note: You can also disable, and then enable a level of authentication. To do this, click the green tick



next to the server name.

8. In the **User settings** section, enter the required field information.

User settings

Create User with an unique E-mail ID

☐

Create User on Authorization Failure

☒

Session Timeout

The following table describes the field information in this section:

Field	Description
Create User an unique E-mail ID	To ensure that every AppViewX user has a unique email ID, turn on this toggle.
Create User on Authorization Failure	To create a user even if authorization fails (but the user is authenticated successfully), turn on this toggle.
Session Timeout	AppViewX lets you set a session timeout limit between 2 and 480 minutes. To set a web session timeout limit, enter the value in minutes.

9. If the AppViewX node password has been changed, in the **Node Settings** section, enter the updated Node Password.

Node settings

Node Password

.....

Save

Cancel



Note: The value entered in the Node Password field should be the same as the node password. To apply the changes, restart the avx-config-server pod in every datacenter.

10. Click **Save**.

Configuring the MFA Settings

MFA is one of the most effective ways to prevent unauthorized access as it requires additional validation of login credentials during a user's authentication process. MFA can be as straightforward as a user providing their password, then entering an accompanying numeric code (OTP) from an Email Text.



Note: For **Onprem** deployment, SMTP configuration should be done before enabling MFA in the settings page. Admin has provision to control MFA feature from the admin role.

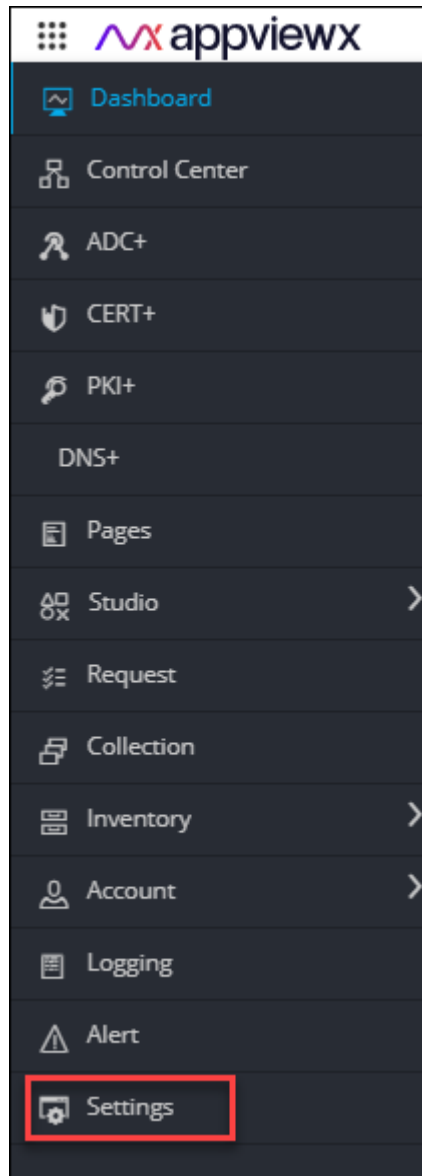
- Admin can Enable/Disable MFA organization level.
- Admin can also give access to enable/disable the MFA feature for the user's profile.



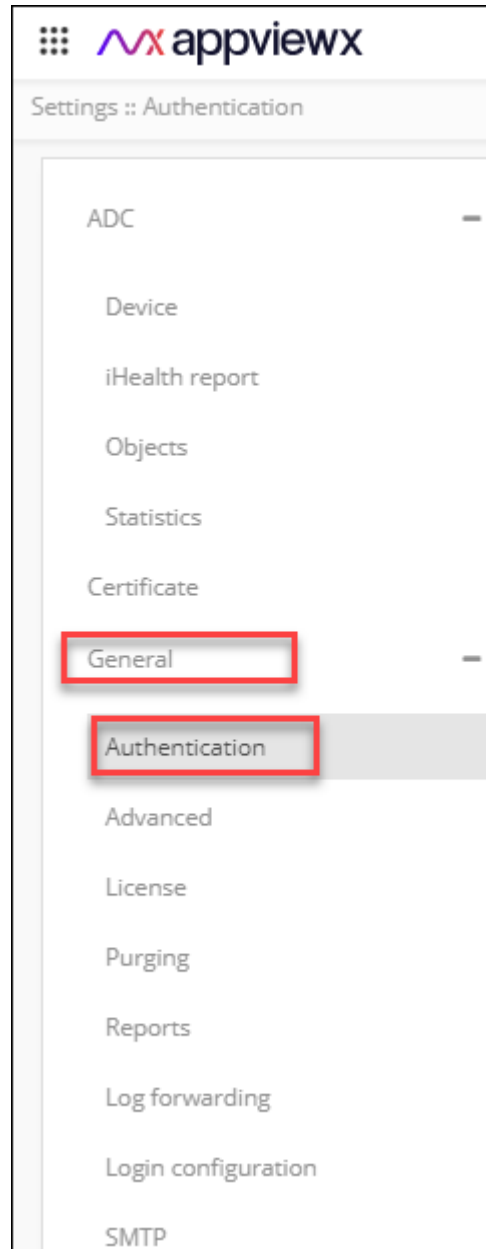
Note: For **SaaS** deployment, MFA is enabled by default for tenant admin user.

To configure the MFA settings:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.

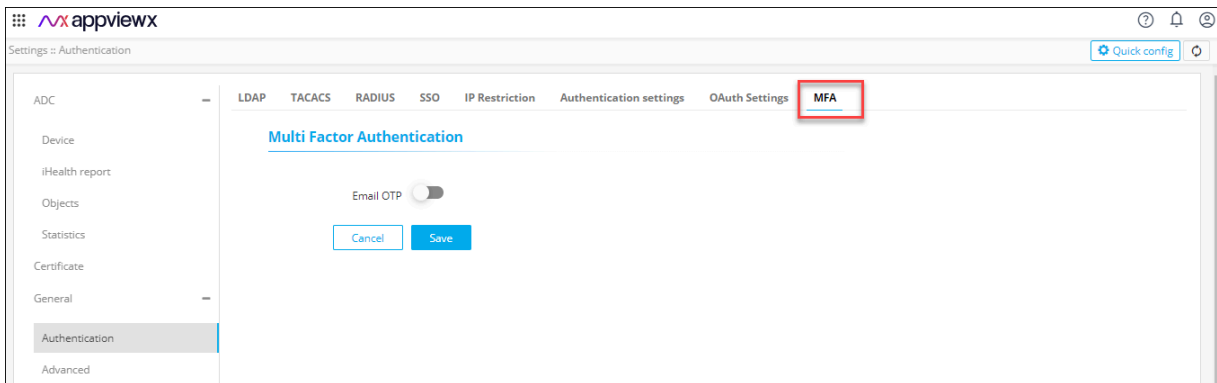


2. From the menu displayed, click **Settings**.
3. On the **Settings** page, from the navigation pane on the left, click **General**.

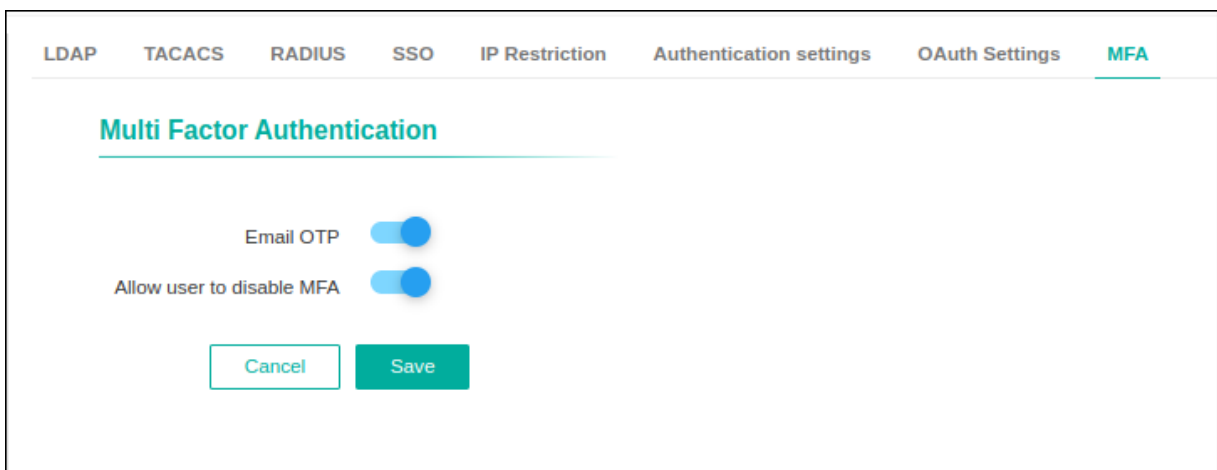


4. Under **General** settings, click **Authentication**.

The **Settings :: Authentication** page is displayed.



5. Click **MFA**, for the Multi Factor Authentication tab.
6. In the **MFA** tab, select **Email OTP** to enable multi factor authentication.
7. On selecting Email OTP, the **Allow user to disable MFA** option appears, which can be enabled or disabled based on the user's requirement.
8. If the admin disables the **Allow user to disable MFA** option, it will enforce MFA usage for all the users. If enabled by the admin, users can enable/disable MFA usage from their user profile settings.



9. To save the **MFA** settings, click **Save**.

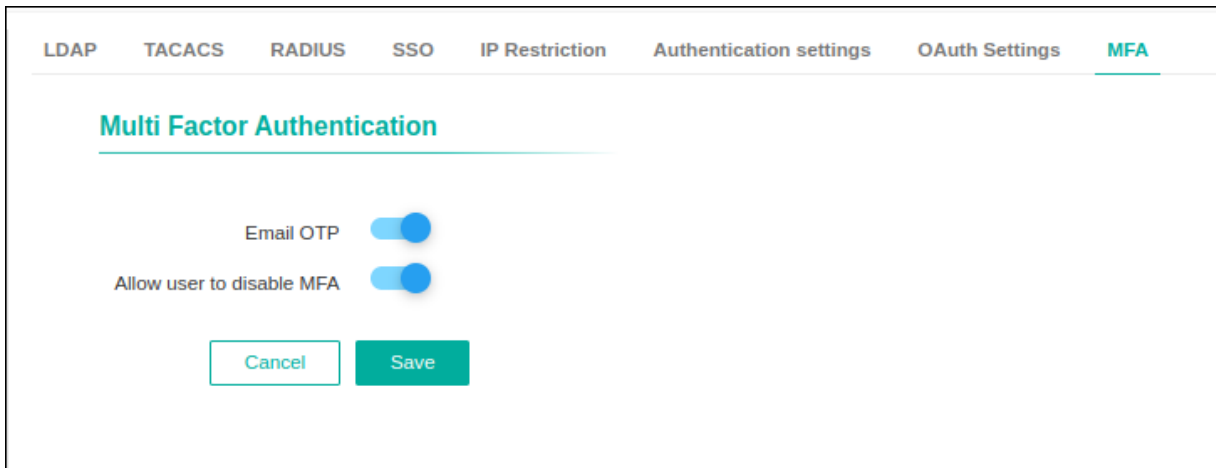
- [MFA Settings for User Profile](#)
- [Logging in using MFA:](#)

MFA Settings for User Profile

Admin has provision to control MFA feature for the user role.

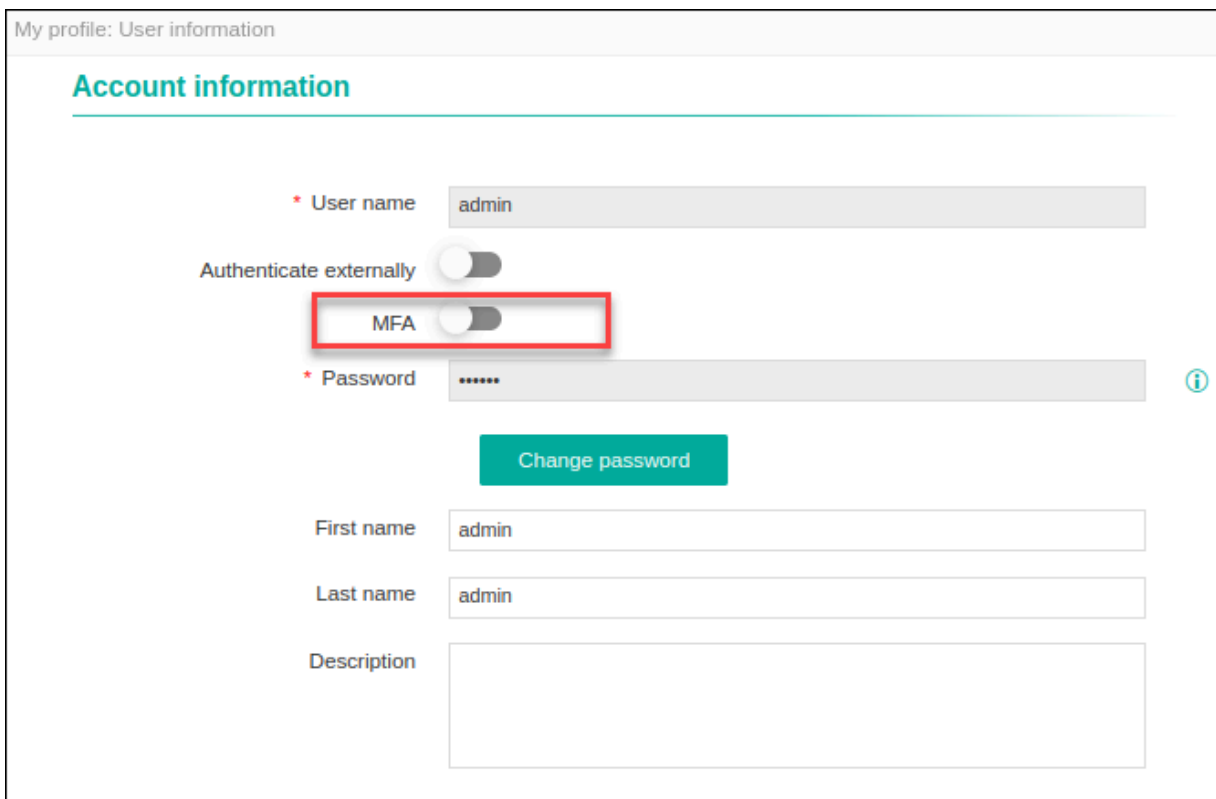
The following steps explain access to enable/disable MFA from user profile:

1. On selecting Email OTP, the **Allow user to disable MFA** option appears.
This can be enabled or disabled based on the user's requirement.



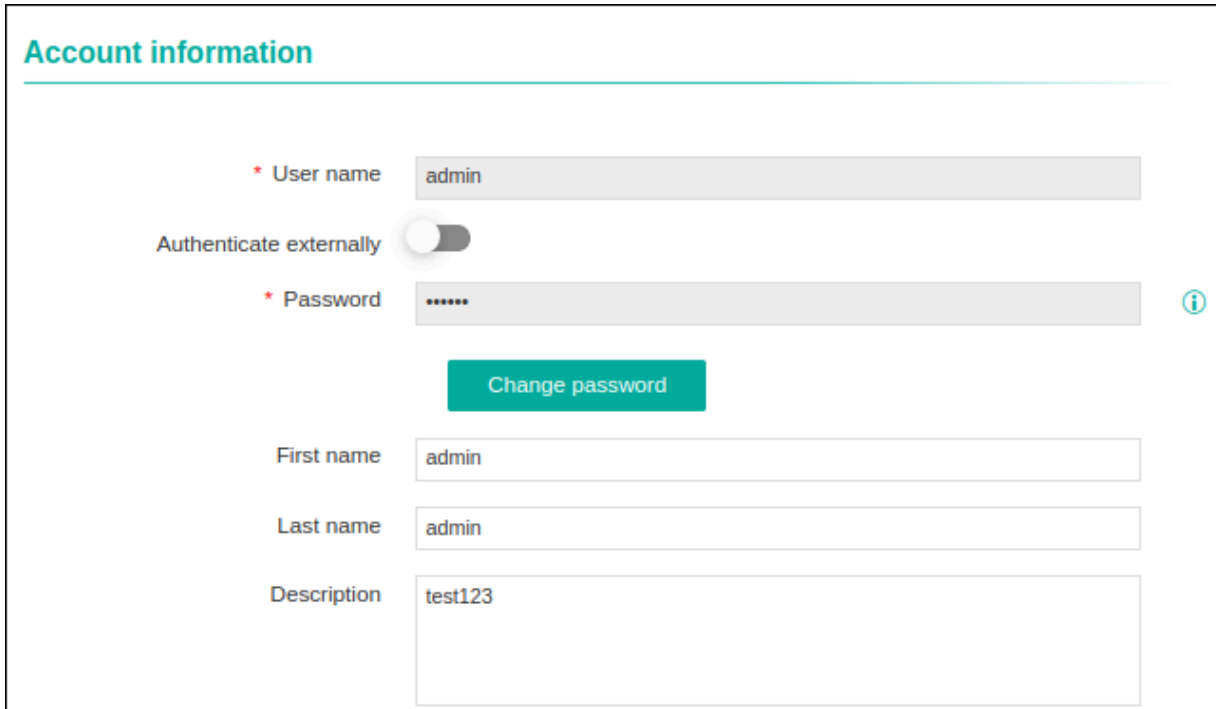
The screenshot shows the 'Multi Factor Authentication' settings page. At the top, there is a navigation bar with tabs: LDAP, TACACS, RADIUS, SSO, IP Restriction, Authentication settings, OAuth Settings, and MFA (which is highlighted). Below the navigation bar, the title 'Multi Factor Authentication' is displayed. Underneath, there are two toggle switches: 'Email OTP' and 'Allow user to disable MFA', both of which are currently turned on. At the bottom of the settings area, there are two buttons: 'Cancel' and 'Save'.

2. If the admin enables **Allow user to disable MFA**, then users have provision to enable/disable MFA and **MFA** option appears in user profile.



The screenshot shows the 'My profile: User information' page. The title 'Account information' is displayed. Below the title, there are several fields and options: 'User name' (admin), 'Authenticate externally' (toggle switch), 'MFA' (toggle switch, highlighted with a red box), 'Password' (masked with dots), 'Change password' button, 'First name' (admin), 'Last name' (admin), and 'Description' (empty text area). An information icon (i) is located next to the password field.

3. If the admin disables **Allow user to disable MFA**, then users can not see **MFA** option in the user profile.



The screenshot shows a user profile form titled "Account information". It contains the following fields and controls:

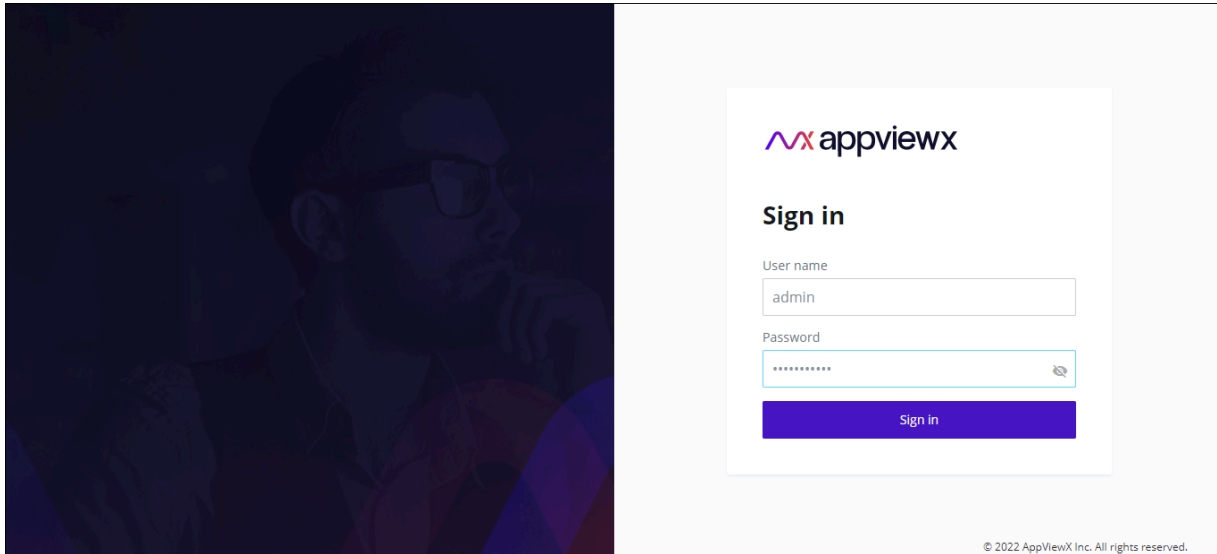
- User name:** A text input field containing "admin".
- Authenticate externally:** A toggle switch that is currently turned off.
- Password:** A text input field containing six dots. To the right of the field is an information icon (i).
- Change password:** A teal button located below the password field.
- First name:** A text input field containing "admin".
- Last name:** A text input field containing "admin".
- Description:** A text input field containing "test123".

Logging in using MFA:

The following steps explain access to AppViewX Login using MFA:

1. Log in using your user credentials (**User name** and **Password**).

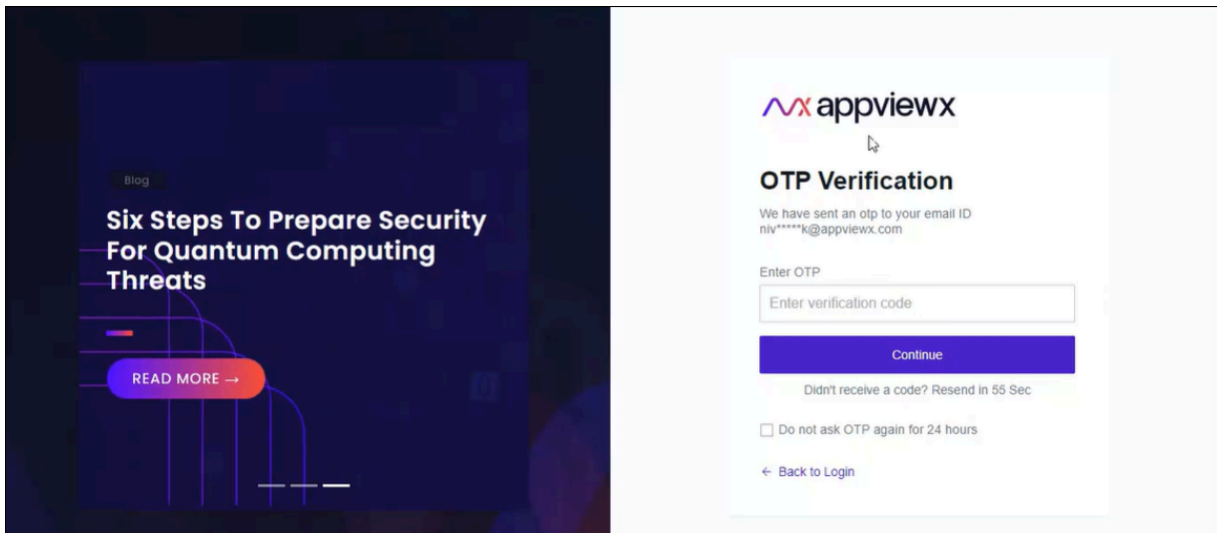
The **AppViewX Sign in page** is displayed.



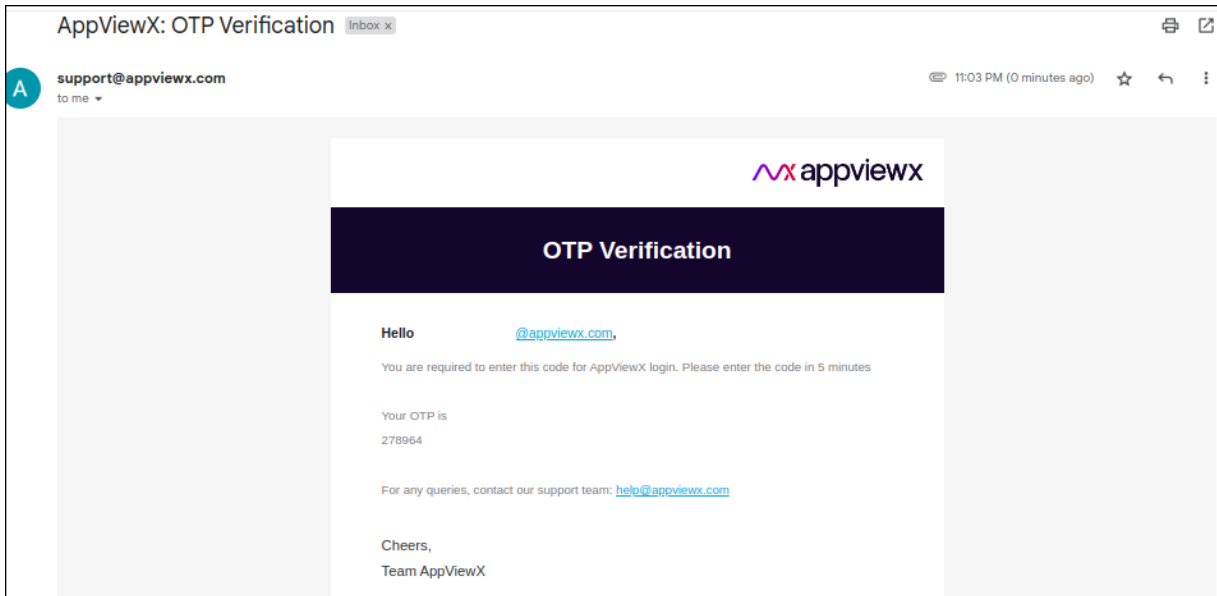
2. Click **Sign in**.

The MFA system generates a random 6 digit numeric value and sends OTP to the registered user's Email ID.

3. User authentication (**OTP Verification**) screen is displayed.



4. Enter OTP which is sent to your registered Email ID.



5. OTP Validation.

- OTP sent to Email will be valid only for next 5 min
- Users will be locked if wrong OTP is entered more than 5 times
- Once the user is locked for 15 min, an auto-generated Email is received asking to contact the administrator to unlock.

6. Resend OTP - MFA.

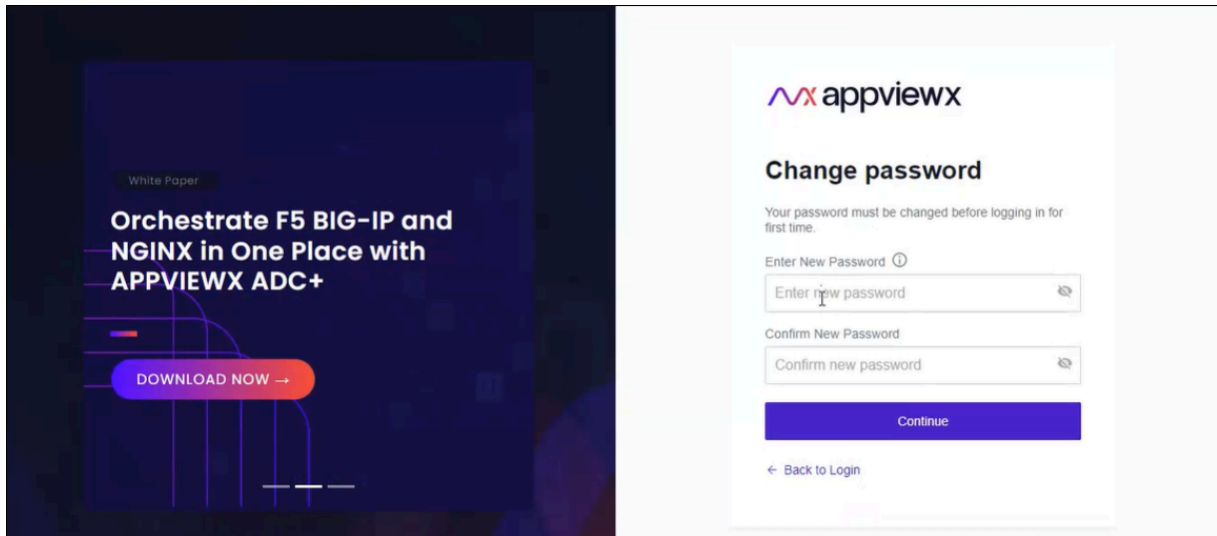
- Resend option will be enabled after **60 seconds**
- Resend option will be available only 5 times for wrong attempt.



Note: Users can select **Do not ask OTP again for 24 hours** during login and disable OTP Verification for next consecutive logins for 24 hours.

7. Click **Continue**.

8. **Change Password** Screen is displayed for the users logging in for the first time.



9. Enter the details in the required fields.

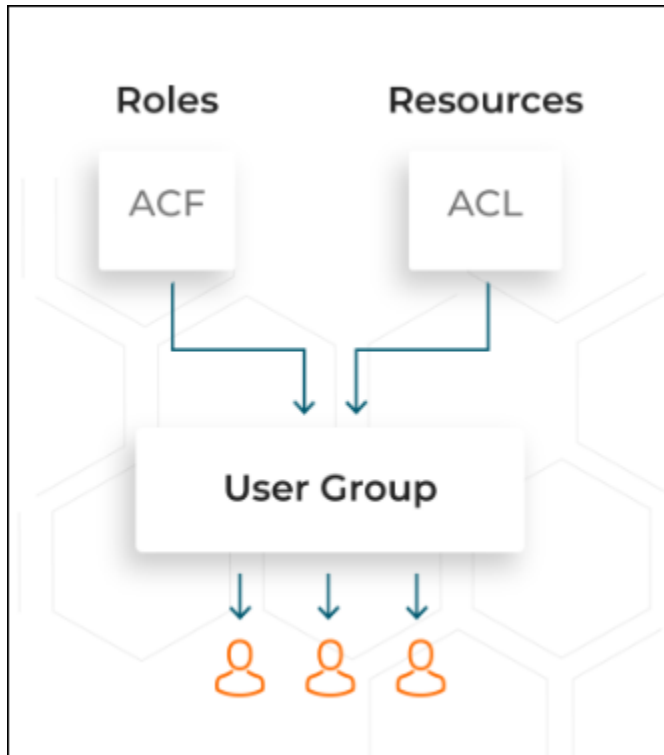
10. Click **Continue**.

Chapter 3: Configuring Role and Resource-Based Access Control

- Overview
- Managing Users
- Service Accounts
- Managing User Groups
- Managing Roles
- RBAC Quick Configuration

Overview

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC). RBAC is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise. It allows you to integrate with the existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and Resources can be customized to suit any organizational structure and user requirements.



RBAC lets employees have access rights only to the AppViewX functions and network resources they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

Benefits of RBAC

Using RBAC should improve operational efficiency, enhance [compliance](#), provide administrators increased visibility, reduction in costs, decrease in risk of [breaches](#), and data leakage.

Managing Users

A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directories (AD).

To create user accounts, you must be assigned the Administrator role. Administrators can define how users should be authenticated to AppViewX. User authentication can either be an internal authentication or external authentication via LDAP, RADIUS, TACACS, and Single Sign-on.



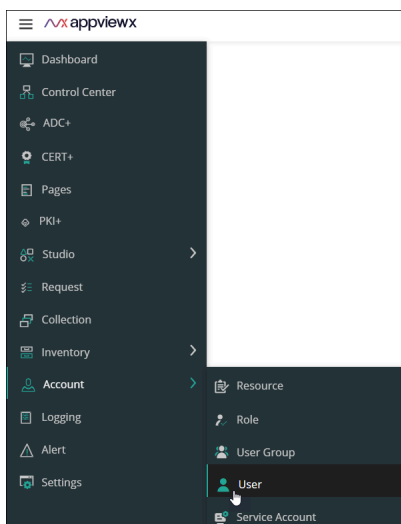
Note: You must add a user to the user group as the roles and resources cannot be directly associated with the user.

- Creating a User
- Modifying a User
- Importing a User
- Enabling a User
- Disabling a User
- Deleting a User

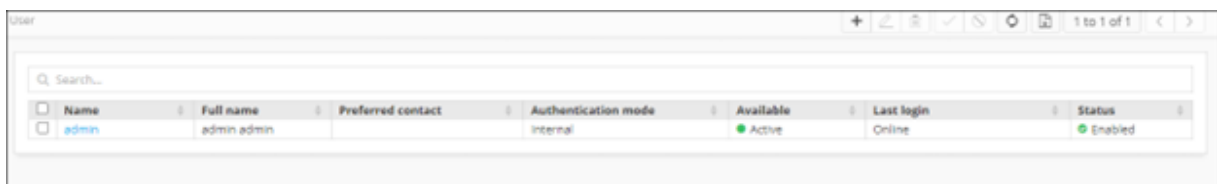
Creating a User

To create a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User**.



The **User** page is displayed.



3. From the top right corner of the screen, click .
4. The **Add** page is displayed, with the **Information** tab open by default.

User > Add

Information User group

Account information

* User name

* Password ⓘ

* Confirm password

Authenticate externally ☐

First name

Last name

Description

Contact information

5. In the **Account Information** section, enter the following details:

Field	Description
*User name	Enter the user name for the new user.
Password	Enter the password for the new user.  Note: The new password should have: • At least one uppercase, lowercase, and numeric character • At least one special character (~!@#\$%^& _-+= ()) • 6 to 24 characters  Note: The new password should not contain: • The user name • The same character more than three times consecutively • Blank spaces
*Confirm Password	Reenter the password for confirmation.
Authenticate externally	To allow authentication by external enterprise servers such as LDAP, TACACS, RADIUS, and so on, select this check box.

Field	Description
	 Note: The Password and Confirm Password fields are disabled if Authenticate externally option is selected.
First name	New user's first name.
Last name	New user's last name.
Description	Descriptive information about the user such as their work location, workgroup, specialty, or any other details.
All * marked fields are mandatory.	

6. In the **Contact Information** section, enter the following details:

Field	Description
*Preferred mode of contact	From the following options, select the user's preferred mode of contact: • Email address • Phone number
*Email address	New user's email address.
*Phone number	New user's phone number.  Note: This field is mandatory only if the preferred mode of contact is Phone number.
All * marked fields are mandatory.	

7. Click **Save**.

8. The user should be assigned or mapped to a user group to be able to log into AppViewX and access the product. To add the user to a group, click the **User group** tab.

Information User group				
Search...				
☐ User Group name	Description	Assigned Roles	Assigned Resources	Status
☐ admin usergroup	Admin user group exists in AppViewX ...	admin	super access	Enabled
Save Cancel				

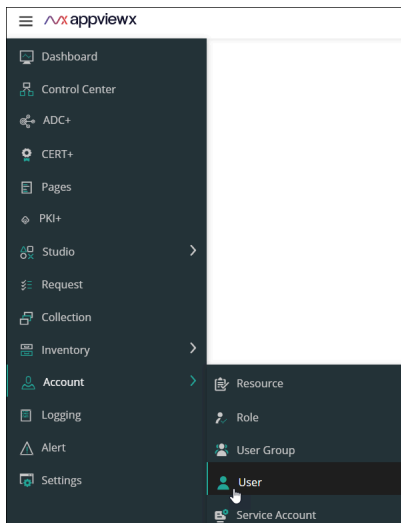
9. To add the user to a group, select the check box for that user group.

10. Click **Save**.

Modifying a User

To modify a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User**.



The **User** page is displayed.

Search...							
☐	Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☐	admin	admin admin		Internal	Active	Online	Enabled

3. From the **User** page, select the check box against the user you want to modify.

Search...							
☐	Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☒	Test		test@abc.com	Internal	Inactive		Enabled
☐	admin	admin admin		Internal	Active	Online	Enabled



4. From the top right corner of the screen, click .
5. The **Modify** page is displayed, with the **Information** tab open by default.

User > Modify :: Test

Information User group

Account information

* User name: Test

Password: ***** ⓘ

Reset password

Authenticate externally ☐

First name:

Last name:

Description:

Contact information

👍

6. In the **Account Information** section, update the required details:

Field	Description
*User name	Enter the user name for the new user.
*Password	Enter the password for the new user.  Note: The new password should have: - At least one uppercase, lowercase, and numeric character - At least one special character (~!@#\$%^*_-= ()) 6 to 24 characters  Note: The new password should not contain: - The user name - The same character more than three times consecutively - Blank spaces
*Confirm Password	Reenter the password for confirmation.
Authenticate externally	To allow authentication by external enterprise servers such as LDAP, TACACS, RADIUS, and so on, select this check box.

Field	Description
	 Note: The Password and Confirm Password fields are disabled if Authenticate externally option is selected.
First name	New user's first name.
Last name	New user's last name.
Description	Descriptive information about the user such as their work location, workgroup, specialty, or any other details.
All * marked fields are mandatory.	

7. In the **Contact information** section, update the required details:

Field	Description
*Preferred mode of contact	From the following options, select the user's preferred mode of contact: • Email address • Phone number
*Email address	New user's email address.
*Phone number	New user's phone number.  Note: This field is mandatory only if the preferred mode of contact is Phone number.
All * marked fields are mandatory.	

8. Click **Save**.

9. To modify the user and user group mapping, by adding a new user group/deleting an existing user group, click the **User group** tab.

Information

User group

Q Search...

☐	User Group name	Description	Assigned Roles	Assigned Resources	Status
☐	admin usergroup	Admin user group exists in AppViewX ...	admin	super access	Enabled

Save

Cancel

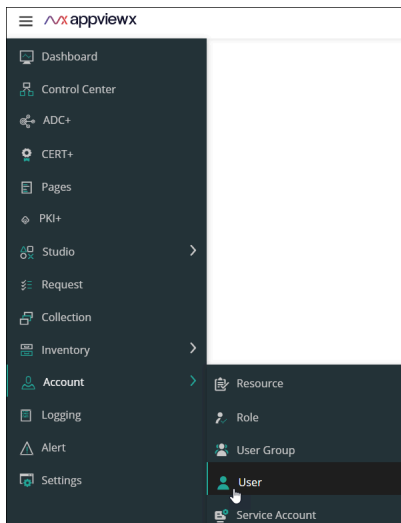
10. To add the user to a group, select the check box for that user group.

11. Click **Save**.

Importing a User

To import users into AppViewX:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User**.



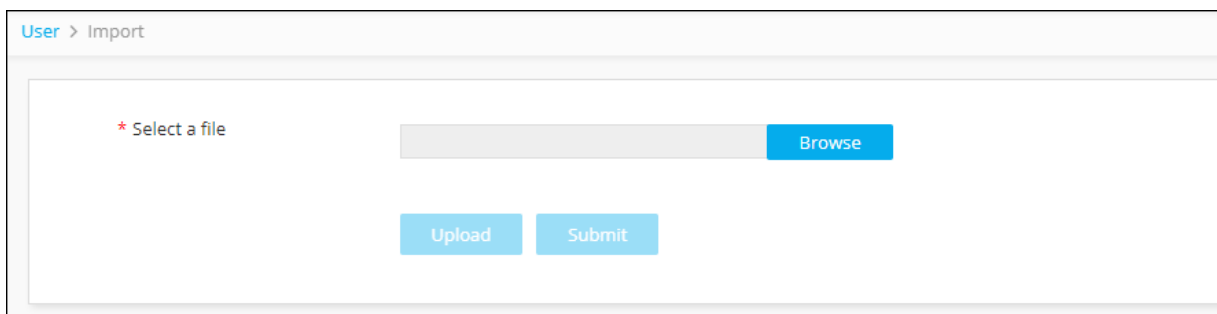
The **User** page is displayed.



Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
admin	admin admin		Internal	Active	Online	Enabled



3. From the top right corner of the screen, click .
4. The **Import** screen is displayed.



User > Import

* Select a file Browse

Upload Submit

5. Click **Browse** and select the user file to upload.



Note: The file must be in .csv format. To download a sample template file click the  icon on the top-right corner.



Tip: The most efficient way to import user details is to download the sample import file that is available by clicking the  (Sample file) icon in the Command bar of the Import screen, modify the contents, save it, and then import it into the system. This reduces the chance of error messages appearing during the import process.

6. Click **Upload** to see the user details displayed in the user interface.



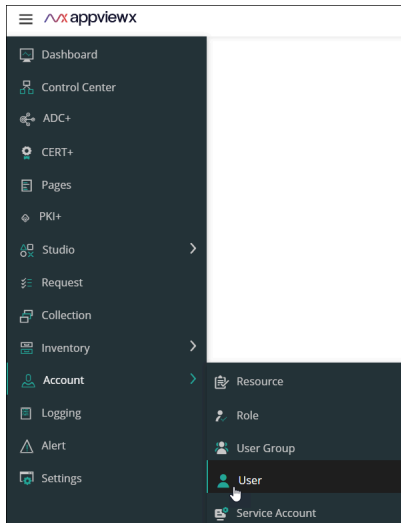
Note: The user details displayed at this point are only for review; the user details have not been imported yet.

7. Review the details of each user in the import file. If you do not want to import specific users, deselect the checkboxes beside their names.
8. Click **Submit**.

Enabling a User

To enable a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User**.



The **User** page is displayed.

Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☐ admin	admin admin		Internal	Active	Online	Enabled

- From the **User** page, select the check box against the user you want to enable.

Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☒ Test		test@abc.com	Internal	Inactive		Enabled
☐ admin	admin admin		Internal	Active	Online	Enabled



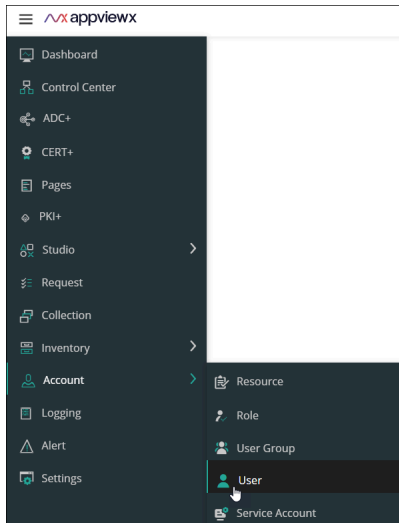
- From the top right corner of the screen, click **Enable**.
- In the **Confirmation** dialog box, click **Yes**.

The selected user is enabled.

Disabling a User

To disable a user:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Account > User**.



The **User** page is displayed.

Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☐ admin	admin admin		Internal	Active	Online	Enabled

- From the **User** page, select the check box against the user you want to disable.

Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☒ Test		test@abc.com	Internal	Inactive		Enabled
☐ admin	admin admin		Internal	Active	Online	Enabled



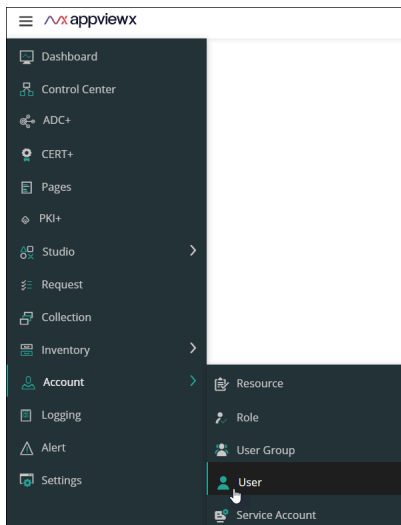
- From the top right corner of the screen, click **Disable**.
- In the **Confirmation** dialog box, click **Yes**.

The selected user is disabled.

Deleting a User

To delete a user:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Account > User**.



The **User** page is displayed.

User						
Search...						
☐	Name	Full name	Preferred contact	Authentication mode	Available	Status
☐	admin	admin admin		Internal	Active	Online

- From the **User** page, select the check box against the user you want to delete.

Search...						
☐	Name	Full name	Preferred contact	Authentication mode	Available	Status
☒	Test		test@abc.com	Internal	Inactive	Enabled
☐	admin	admin admin		Internal	Active	Online



- From the top right corner of the screen, click **Delete**.
- In the **Confirmation** dialog box, click **Yes**.

The selected user is deleted.

Service Accounts

The service account is a special type of account intended to represent a non-human user. API endpoints will be consumed by non-human users. For example, automated applications are used to perform some operations. So, AppViewX introduced a new account type called Service Account. Using this, API endpoints can be accessed using OAuth based authentication.

- [Client Credentials Grant Type](#)
- [Managing Service Account](#)

- [Configuring OAuth Settings](#)
- [OAuth](#)
- [OAuth Workflow](#)

Client Credentials Grant Type

Client Credential Grant type is one of the grant types supported by OAuth 2.0. A Service Account is provided with a Client ID and Client Secret. Then, you can use this Client ID and Client Secret in client applications to get an Access token and perform API actions using the Access Token.

Managing Service Account

To configure managing service accounts, follow the below steps:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.

2. From the menu displayed, click **Account > Service Account**.

The screenshot below shows an existing Service Account. The secret is hidden by default. The client credentials can be copied using the corresponding copy buttons. The Client ID and Client Secret can be regenerated anytime using the corresponding regenerate buttons. When a Client ID is regenerated, the corresponding Client Secret is also regenerated. The Access tokens generated by the previous set of Client ID and Client Secret will still work until the token gets expired.

Service Account > Modify :: Application_1

Information User Group

Account Information

* Name: Application_1

* Client Id: 0f34e848-f069-4cfb-820e-3dc53b3019fc  

Client Secret:

 Show  Regenerate  Copy Secret

Description: Application_1

Contact Information

* Email Address: testuser15@appviewx.com

3. To define the access privileges and scope for this service account, assign the required User Groups to this account.

Service Account > Modify :: Application_1

Information **User Group**

Search: 1 to 2 of 2 < > 

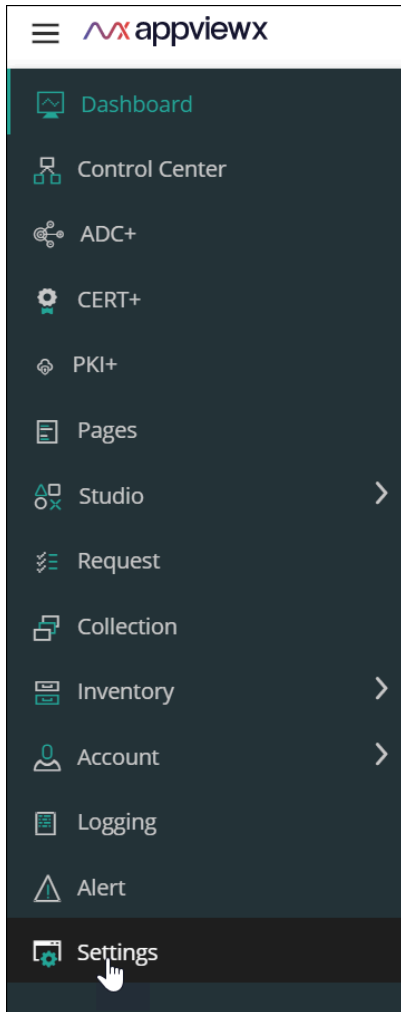
☐	User Group name	Description	Assigned Roles	Assigned Resources	Status
☒	admin usergroup	Admin user group exists in AppViewX...	admin	super access	Enabled
☐	testGroup		roleTest		Enabled

 Save  Cancel

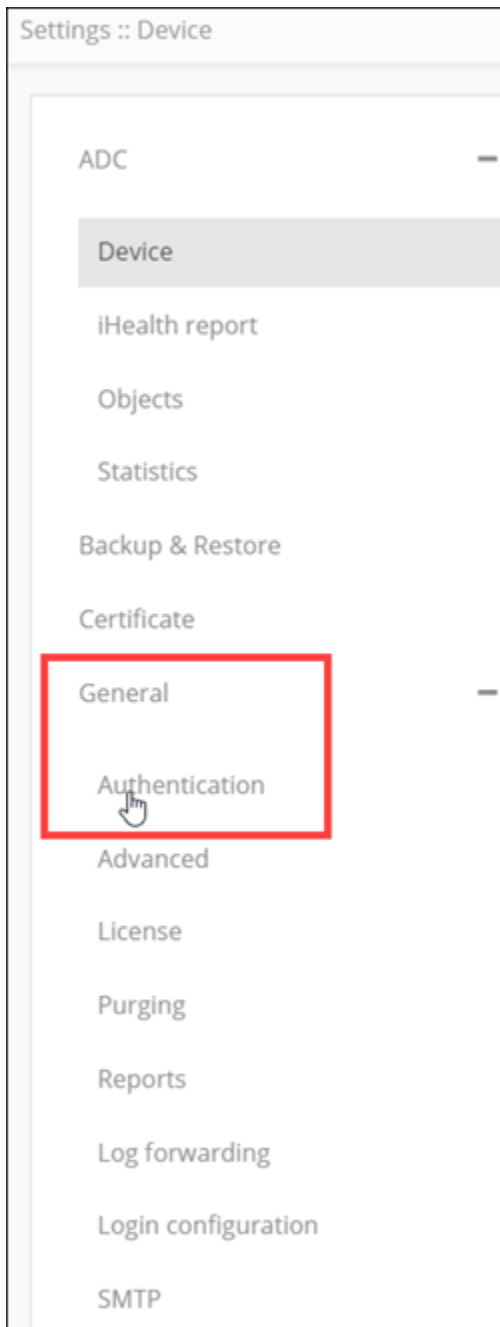
Configuring OAuth Settings

To configure OAuth settings, follow the below steps:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

Settings :: Authentication

Quick config 0 Entries

ADC

LDAP TACACS RADIUS SSO IP Restriction Authentication settings OAuth Settings

Device

Health report

Objects

Statistics

Backup & Restore

Certificate

General

Authentication

Advanced

License

Purging

Reports

Log forwarding

Login configuration

SMTP

General information

* Host

* Port 389

LDAPS

Upload certificate

Bind DN CN=admin,DC=example,DC=com

Bind password

Data center dc1

Authorization

Enable Nested Groups

LDAP Sync

5. To define the validity of Access Token and Client Secret from AppViewx, on the **Settings :: Authentication** page, click **OAuth Settings**.

ADC

LDAP TACACS RADIUS SAML IP Restriction Authentication settings **OAuth Settings**

Device

Health report

Objects

Statistics

Backup & Restore

Certificate

General

Authentication

Advanced

License

Purging

Reports

* Client Secret validity 180 Days

* Access Token Validity 30 Minutes

Save Cancel



Note: By default, Client Secret expires in 180 days and the Access token expires in 30 Minutes. It is customizable.



Note: Whenever an Access Token expires, an HTTP Error Code 401 is displayed in the API response. The client application can generate a new Access Token using the Client ID and Client Secret.



Note: When the Client Secret expires, you can regenerate a new Client Secret from AppViewX in **Account > Service Account > Account Name > Client Secret > Regenerate**.

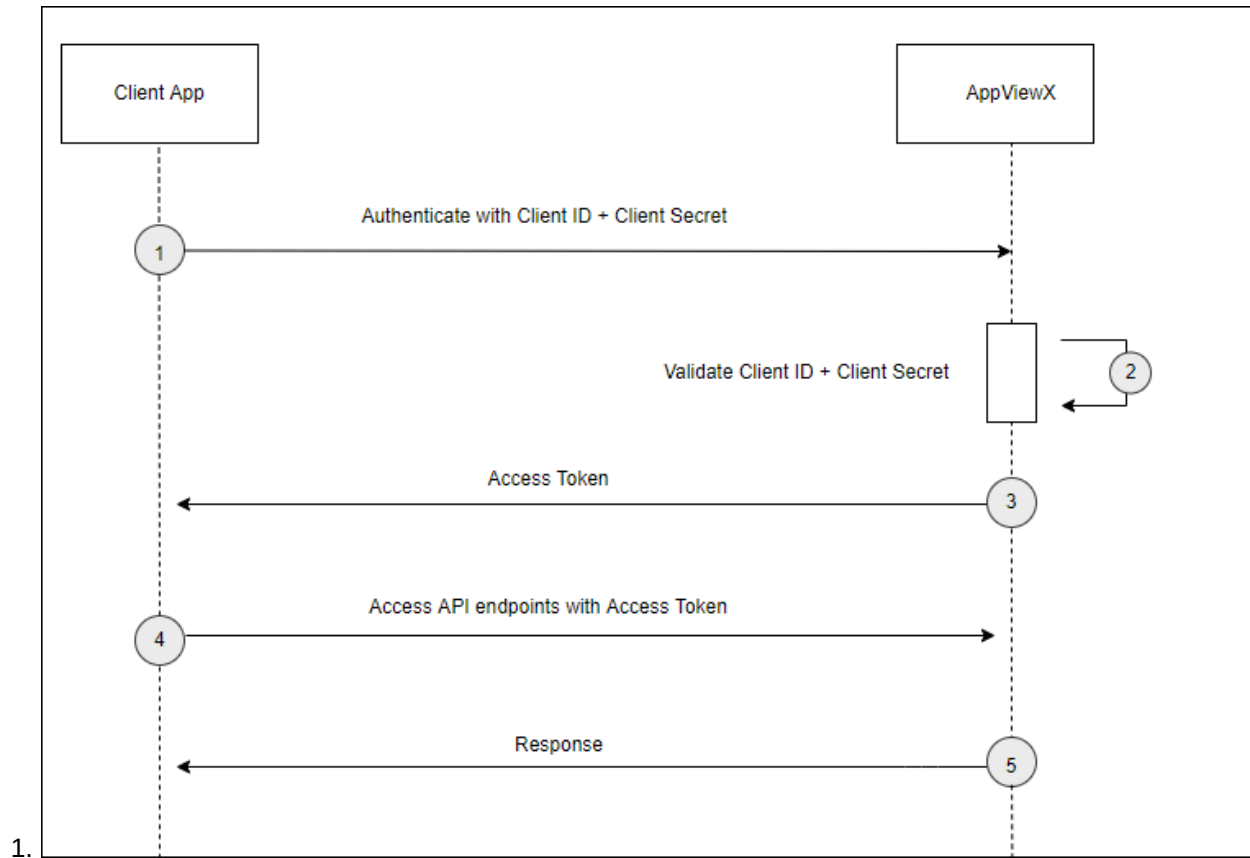
oAuth

OAuth is a standard that applications can use to provide the client applications with **secure delegated access**. Using OAuth, access to client applications is delegated without sharing the password credentials.

AppViewX can be managed using web console and API endpoints.

To improve the security of the API endpoints access, AppViewX has introduced the OAuth Client Credentials Grant Type.

oAuth Workflow



Client application sends a request to the AppViewX server with a Client ID and Client Secret to get the Access Token.

API: acctmgmt-get-service-token

URL: <http://localhost:5300/avxapi/acctmgmt-get-service-token?gwsource=web&gwkey=f000ca01>

Method: POST

Header:

Basic Authentication : (base64(clientId:clientsecret))

Payload:

```
{
  "payload": {
    "grant_type": "client_credentials"
  }
}
```

}

2. AppViewX validates the Client ID and the Client Secret.
3. Once the Client ID and the Client Secret are validated by AppViewX, it then returns the Access token with the expiry time. This is a JWT token. The client application can decode this JWT token to get all the claims including the expiry time of that token inside the exp claim.

Response:

```
{
  "response":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWUiOiJBcHBsaWNhdGlubl8xliwiYXVkljoiYXZ4IiwiaY2xpZW50SWQiOiIwZjM0ZTg0OC1mMDY5LTRjZmItOElwZS0zZGM1M2IzMDE5ZmMiLCJpc3MiOiJhdngiLCJleHAiOiJlE2NDMxMDE3OTQ3ImlndyYW50IHR5cGUiOiJjbGllbnRfY3JlZGVudGlhbHMifQ.EC6my35MCUsMVC0gsylFqWVzqjgs5Js87Owf1esoano",
  "message": null,
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```

Access Token JWT Claims:

```
{
  "sub": "Application_1",
  "aud": "avx",
  "clientId": "0f34e848-f069-4cfb-820e-3dc53b3019fc",
  "iss": "avx",
  "exp": 1643107794,
  "grant type": "client_credentials"
}
```

4. The Client application then accesses the API endpoints with the Access Token in the “**token**” header of the API. Then AppViewX provides the response.

Example

Refer to the below sample screenshot for reference.

The screenshot shows a REST client interface for a request titled "acctmgmt-fetch-acf-role-permission".

Request Details:

- METHOD:** GET
- URL:** `https://${"host"}:${"port"}/v1/api/acctmgmt-fetch-acf-role-permission?apikey=f000ca016&resource=api`
- HEADERS:**
 - ☐ sessionid: `${"sessionid"}`
 - ☒ token: `${"token"}`

Response Details:

- Status:** 200
- Headers:**

```

status: 200
x-dns-prefetch-control: off
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=15552000; includeSubDomains
x-download-options: noopen
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
x-jwt-timestamp: 1639662195361
date: Thu, 16 Dec 2021 13:43:25 GMT +4w
appviewnode: avx-platform-core-67b97477b9-8fvtz:8021
loginmethod: api
content-type: application/json
x-envoy-upstream-service-time: 80

```
- Body:**

```

{
  "response": {
    "tenant": "default",
    "rolePermissionMap": {
      "certificate:settings:casettings:custom_ca": ["admin", "CA Manager"],
      "certificate:connectorActions:secureConnector": ["admin"],
      "certificate:settings:appsettings:view": ["CLM Manager", "admin", "Appli", "adc:dashboard"]
    }
  }
}

```

Managing User Groups

A user group is a set of individual users assigned with the same roles and resources. You can associate one or more roles and resources to a user group. Users within that user group are granted the role and resource permissions.



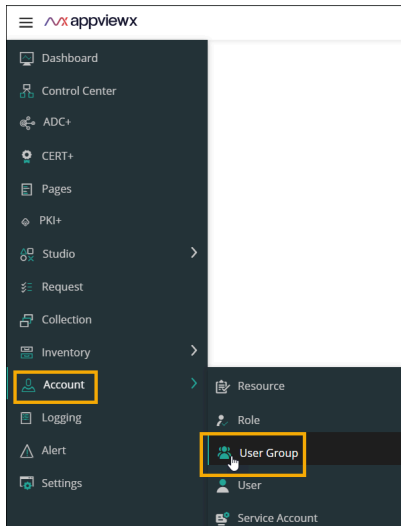
Note: You can associate roles and resources only with user groups.

- [Creating a User Group](#)
- [Cloning a User Group](#)
- [Modifying a User Group](#)
- [Enabling a User Group](#)
- [Disabling a User Group](#)
- [Deleting a User Group](#)

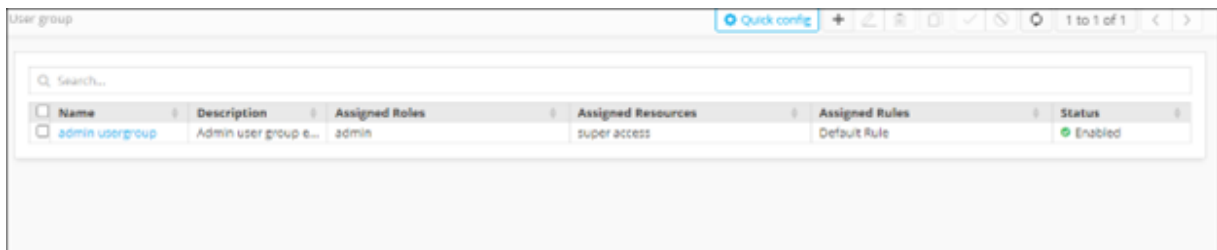
Creating a User Group

To create a user group:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, select **Account > User Group**.



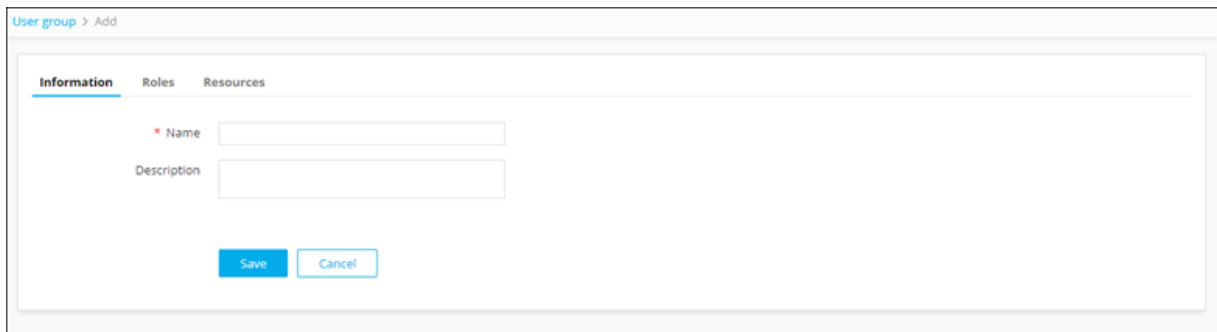
The **User Group** page is displayed.



Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled



3. From the top right corner of the screen, click .
4. The **Add** page is displayed, with the **Information** tab open by default.



User group > Add

Information Roles Resources

* Name

Description

Save Cancel

5. Enter the following details:

Field	Description
*Name	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).
All * marked fields are mandatory.	

6. Click **Save**.

7. To assign roles to this user group, in the **Roles** tab, select the check boxes against the required roles.

Information Roles Resources			
Q Search...			
☐ Role name	Description	Status	
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code...	Enabled	
☒ Executive Director-ADC	AppViewX provides organisations with holistic, business-level vi...	Enabled	
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out o...	Enabled	
☐ Application User	Responsible to monitor the application specific certificates, set...	Enabled	
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled	
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level vi...	Enabled	
☐ Application Manager-ADC	Responsible for managing technical aspects of one or more maj...	Enabled	
☒ Application Manager-Cert	Responsible to manage the application specific certificates and ...	Enabled	
☐ admin	admin	Enabled	
☐ Executive Director-Cert	AppViewX provides organizations with holistic, business-level vi...	Enabled	
☐ Traffic Manager	Responsible to perform traffic management operations and Mo...	Enabled	
☐ USERS/Read-Only Admins	This role grants users complete access to all objects on the syst...	Enabled	
☒ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled	
☐ DevOps Manager	Responsible for managing a DevOp team; they may write applic...	Enabled	
☐ CA Manager	Responsible to manage CA related request and operations in A...	Enabled	
☐ Security Manager	This role grants users complete access to all objects on the syst...	Enabled	
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level vi...	Enabled	



Note: A user group can be assigned to more than one role and resource in the system. A user assigned to a user group with more than one role or resource has all of the permissions of all of the roles and resources to which he or she is assigned. If one resource has only Read access to a component and another resource has Read/Write access to the same component, the higher-level access permissions (Read/Write) take precedence and the user has Read/Write access.

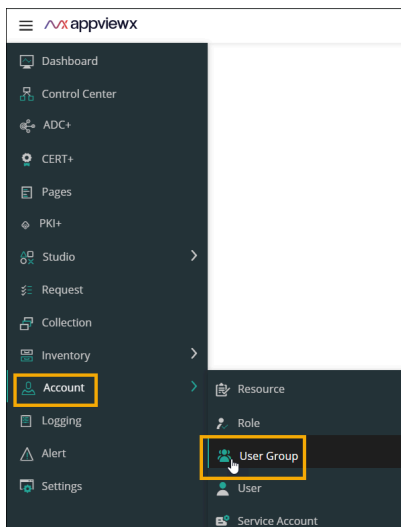


Note: Admins who associate User Groups to Roles and Resources may skip/forget to associate User Groups to a user. To overcome this, an alert icon has been added to the User Group inventory to notify if the group is not associated with a role, resource, or both.

Cloning a User Group

To clone a user group:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, select **Account > User Group**.



The **User Group** page is displayed.

User group					
Quick config Search...					
☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules
☐	admin usergroup	Admin user group e...	admin	super access	Default Rule
Status: Enabled					

3. From the **User Group** page, select the user group you want to clone.

User group					
Quick config Search...					
☒	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules
☒	admin usergroup	Admin user group e...	admin	super access	Default Rule
Status: Enabled					



4. From the top right corner of the screen, click **Clone**.

5. The **Cloning** page is displayed, with the **Information** tab open by

The screenshot shows a web form titled 'User group > Add'. It has three tabs: 'Information', 'Roles', and 'Resources'. The 'Information' tab is active. It contains two input fields: 'Name' (with a red asterisk indicating it is mandatory) and 'Description'. At the bottom of the form are two buttons: 'Save' (in blue) and 'Cancel' (in light blue).

default.

6. Update the required details:

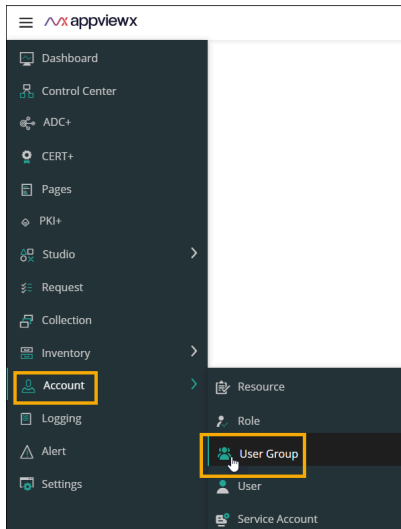
Field	Description
*Name	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).
All * marked fields are mandatory.	

7. Click **Save**.

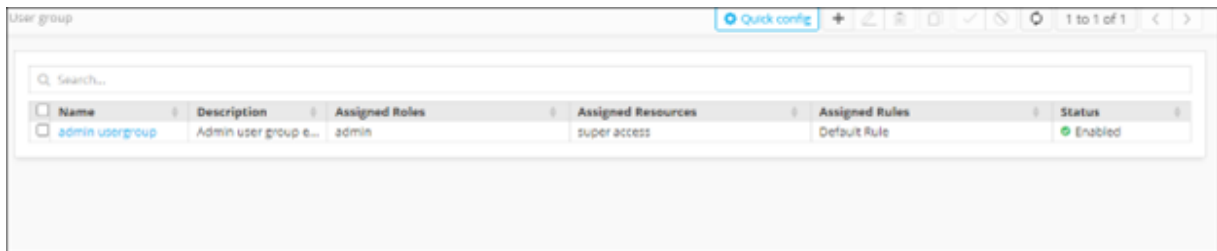
Modifying a User Group

To create a user group:

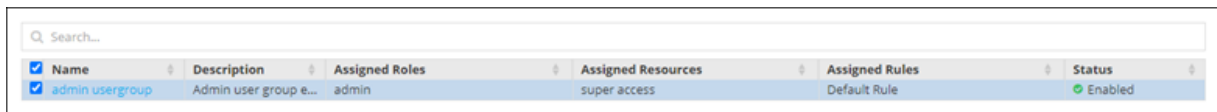
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, select **Account > User Group**.



The **User Group** page is displayed.

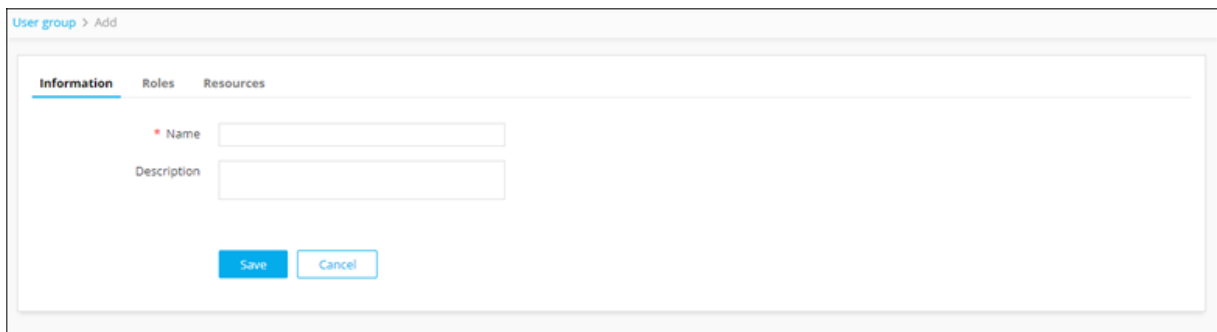


3. From the **User Group** page, select the user group you want to modify.



4. From the top right corner of the screen, click **Modify**.

5. The **Modify** page is displayed, with the **Information** tab open by default.



6. Update the required details:

Field	Description
*Name	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).
All * marked fields are mandatory.	

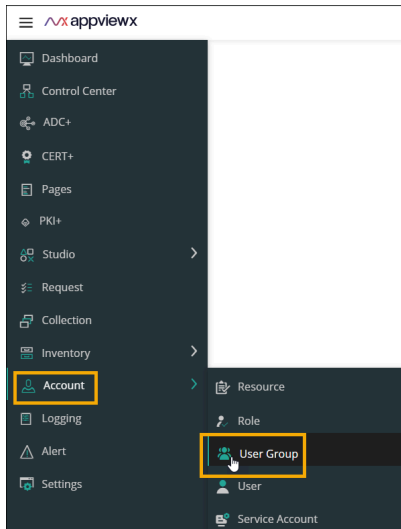
- Click **Save**.
- To modify the role assignment for this user group, in the **Roles** tab, select/clear the check boxes against the required roles and resources

Information Roles Resources		
Q Search...		
☐ Role name	Description	Status
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code...	Enabled
☒ Executive Director-ADC	AppViewX provides organisations with holistic, business-level vi...	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out o...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, set...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level vi...	Enabled
☐ Application Manager-ADC	Responsible for managing technical aspects of one or more maj...	Enabled
☒ Application Manager-Cert	Responsible to manage the application specific certificates and ...	Enabled
☐ admin	admin	Enabled
☐ Executive Director-Cert	AppViewX provides organizations with holistic, business-level vi...	Enabled
☐ Traffic Manager	Responsible to perform traffic management operations and Mo...	Enabled
☐ USERS/Read-Only Admins	This role grants users complete access to all objects on the syst...	Enabled
☒ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applic...	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in A...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the syst...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level vi...	Enabled

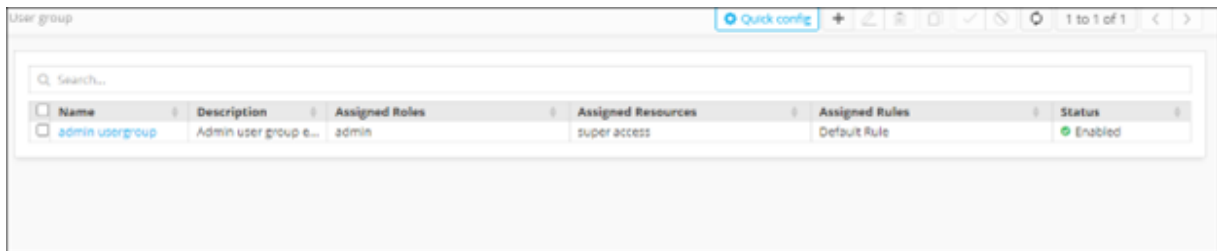
Enabling a User Group

To enable a user group:

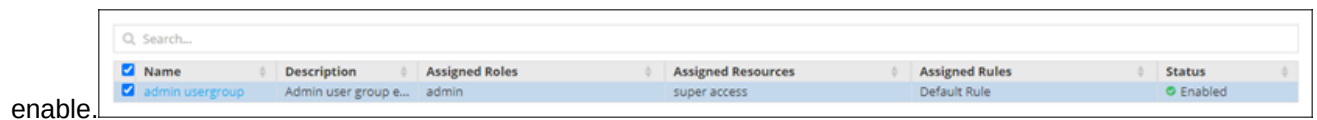
- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, select **Account > User Group**.



The **User Group** page is displayed.



- From the **User Group** page, select the user group you want to



enable.

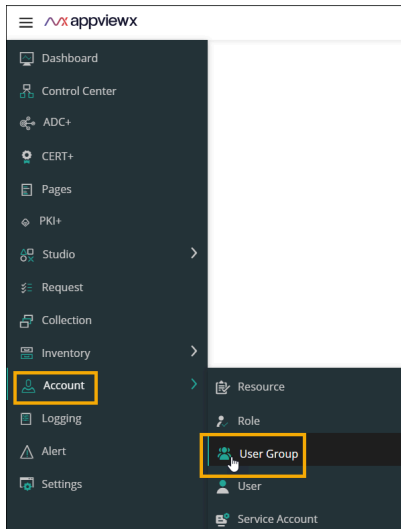


- From the top right corner of the screen, click
- In the **Confirmation** dialog box, click **Yes**.

Disabling a User Group

To disable a user group:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, select **Account > User Group**.



The **User Group** page is displayed.

User group						
Search...						
☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☐	admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled

3. From the **User Group** page, select the user group you want to disable.

User group						
Search...						
☒	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☒	admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled



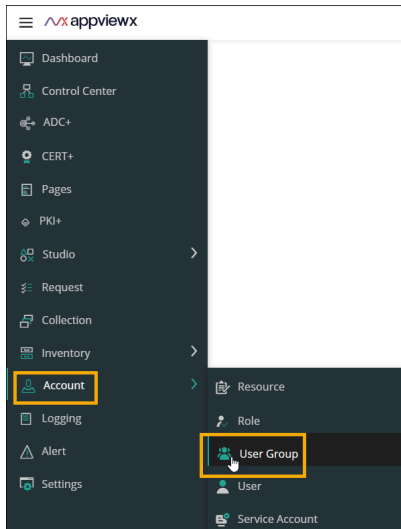
4. From the top right corner of the screen, click **Disable**.

5. In the **Confirmation** dialog box, click **Yes**.

Deleting a User Group

To delete a user group:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, select **Account > User Group**.



The **User Group** page is displayed.

User group						
Search...						
☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☐	admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled

3. From the **User Group** page, select the user group you want to delete.

User group						
Search...						
☒	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☒	admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled



4. From the top right corner of the screen, click

5. In the **Confirmation** dialog box, click **Yes**.

Managing Roles

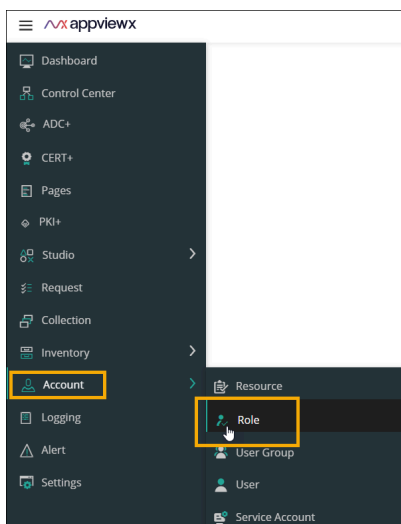
A set of permissions to execute specific tasks in the application is termed as Roles in AppViewX. Roles can be assigned only to a user group. Users within user groups will inherit role permissions assigned to that group. User groups can be assigned more than one role. A default set of roles is available within the application as per the industry standards.

- Creating a Role
- Cloning a Role
- Modifying a Role
- Enabling a Role
- Disabling a Role
- Deleting a Role

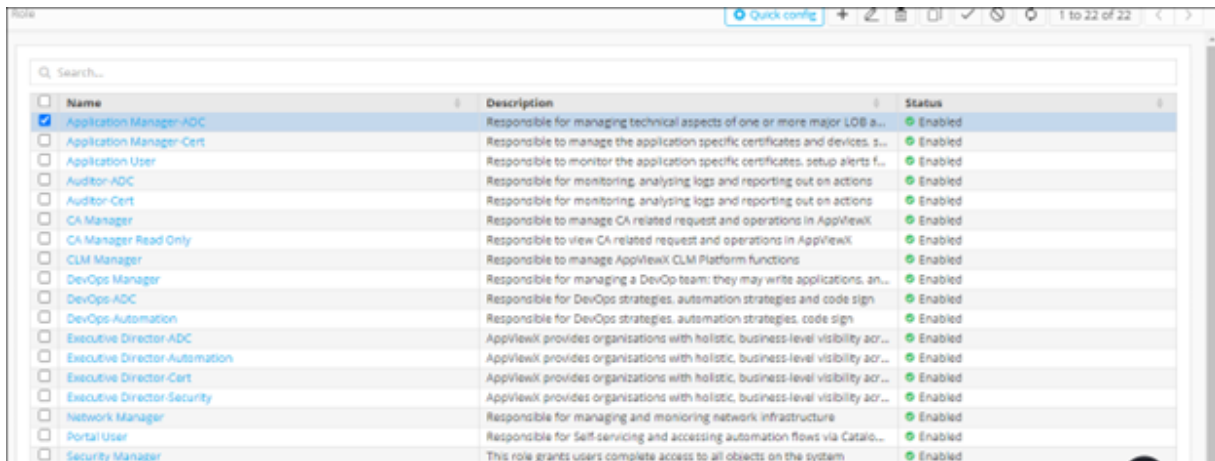
Creating a Role

To create a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, select **Account > Role**.



The **Role** page is displayed.

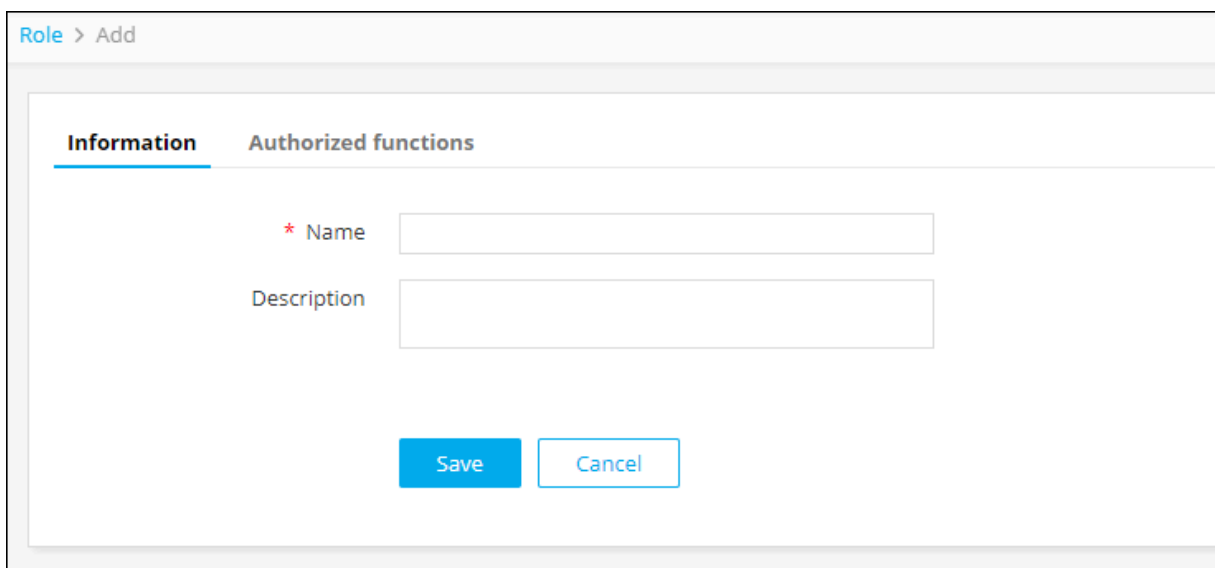


Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices, s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled



3. From the top right corner of the screen, click .

The **Add** page is displayed.



Role > Add

Information

Authorized functions

* Name

Description

Save

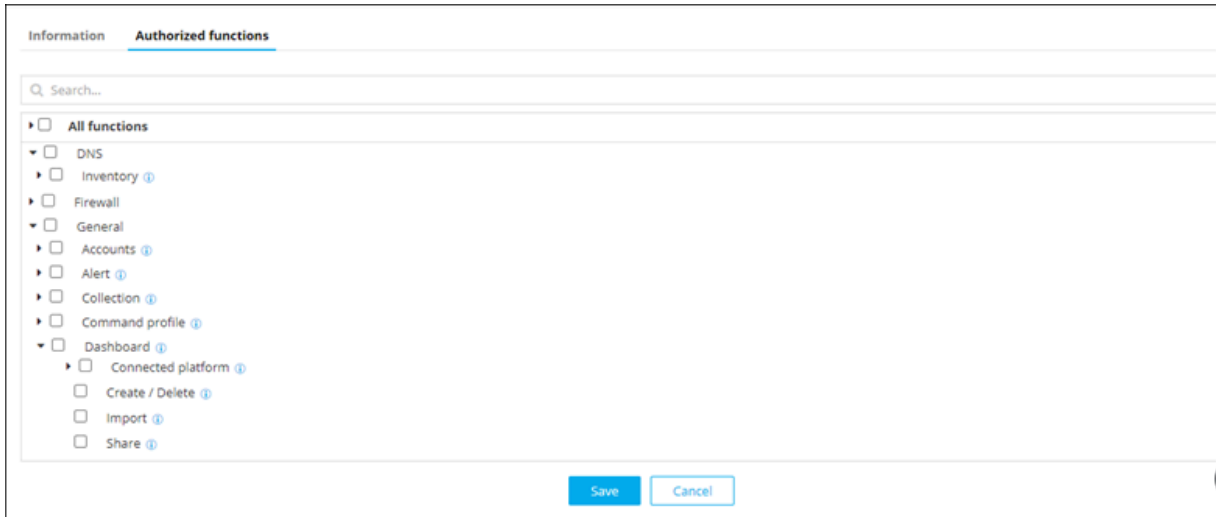
Cancel

4. Under the **Information** tab, enter the following details:

Field	Description
*Name	Name of the role.
Description	Role/features/functionalities associated with the role.
All * marked fields are mandatory.	

5. Click **Save**.

6. In the **Authorized functions** section, select the checkbox beside the functionalities that you want to associate with the role.
7. To assign functions at a granular level, click the  icon for the functions' check box and then select individual sub-options within the functions.



8. Click **Save**.

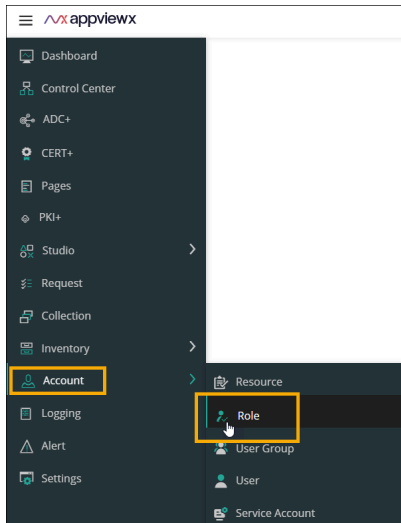
Details of the new role are displayed in the list on the **Role** page.

Cloning a Role

Cloning lets you create a copy of an existing role with a different name. You can modify the permissions and tasks that can be performed while cloning a role.

To clone a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.



The **Role** page is displayed.

Quick config		
1 to 22 of 22		
☐	Name	Description
☒	Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...
☐	Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...
☐	Application User	Responsible to monitor the application specific certificates, setup alerts f...
☐	Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions
☐	Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions
☐	CA Manager	Responsible to manage CA related request and operations in AppViewX
☐	CA Manager Read Only	Responsible to view CA related request and operations in AppViewX
☐	CLM Manager	Responsible to manage AppViewX CLM Platform functions
☐	DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...
☐	DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign
☐	DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign
☐	Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Network Manager	Responsible for managing and monitoring network infrastructure
☐	Portal User	Responsible for Self-servicing and accessing automation flows via Catale...
☐	Security Manager	This role grants users complete access to all objects on the system

- For the role you want to clone, select the corresponding check box.



- From the top right corner of the screen, click
- In the **Information** section, enter a new **Name** for the role.

The screenshot shows a web interface with two tabs: 'Information' (active) and 'Authorized functions'. Under the 'Information' tab, there is a form with the following elements:

- A red asterisk (*) followed by the label 'Name' and an empty text input field.
- The label 'Description' followed by a text area containing the text: 'Responsible for managing technical aspects of one or more major LOB applications.'
- At the bottom, there are two buttons: 'Save' (solid blue) and 'Cancel' (outlined blue).

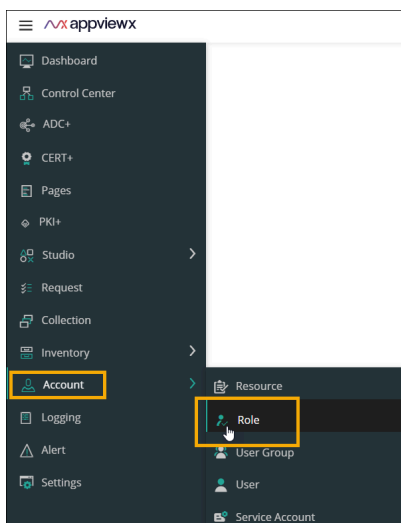
6. Click **Save**.

The selected role is cloned.

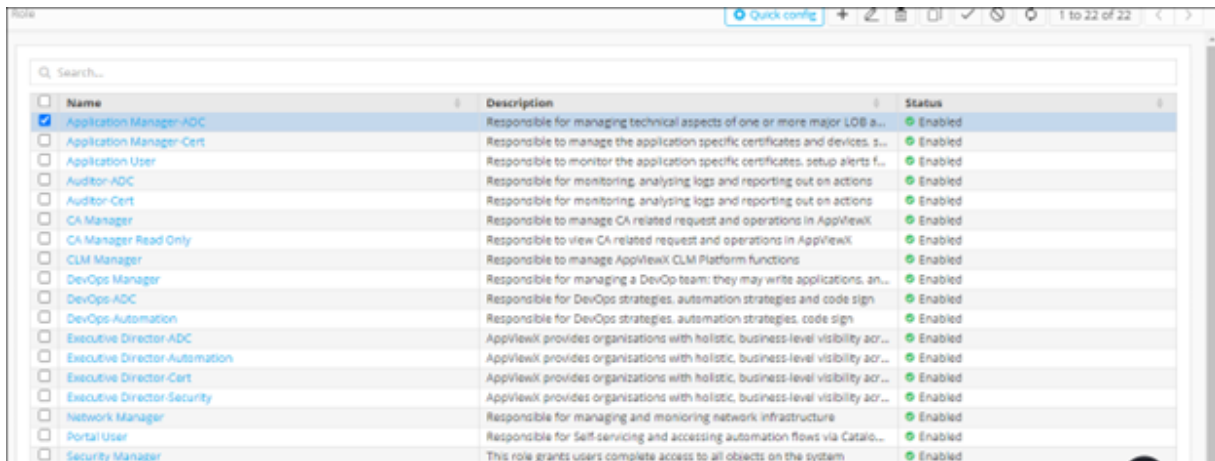
Modifying a Role

To modify a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account > Role**.



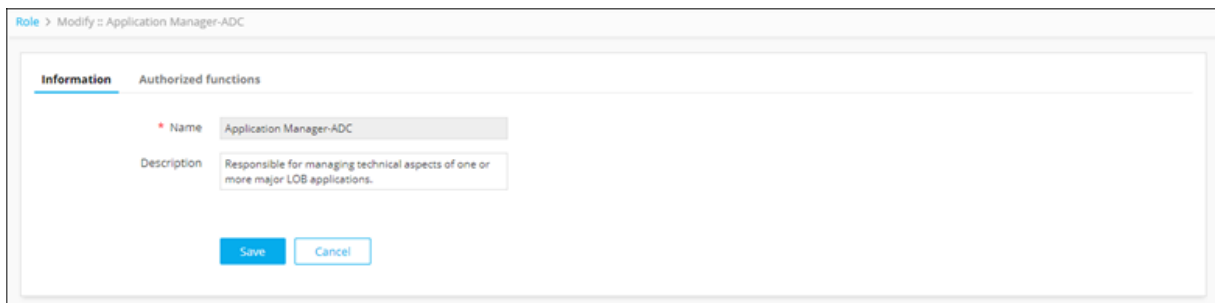
The **Role** page is displayed.



Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled



- From the top right corner of the screen, click **Modify**.
- The **Modify :: Application Manager-ADC** page is displayed (because we selected the Application Manager role).
- Modify the details in the **Information** and **Authorized functions** as required.



Role > Modify :: Application Manager-ADC

Information Authorized functions

Name: Application Manager-ADC

Description: Responsible for managing technical aspects of one or more major LOB applications.

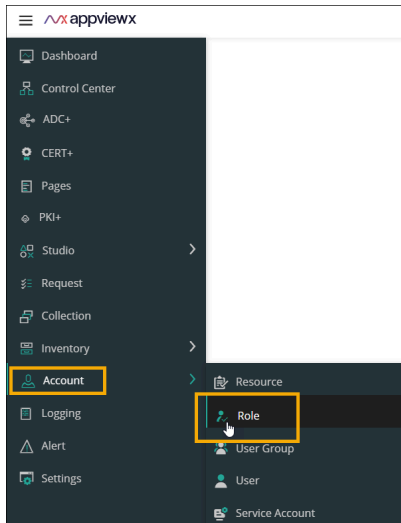
Save Cancel

- Click **Save**.
- The selected role is modified.

Enabling a Role

To enable a role:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Account > Role**.



The **Role** page is displayed.

Quick config		
1 to 22 of 22		
Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catala...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled

- For the (disabled) role you want to enable, select the corresponding check box.



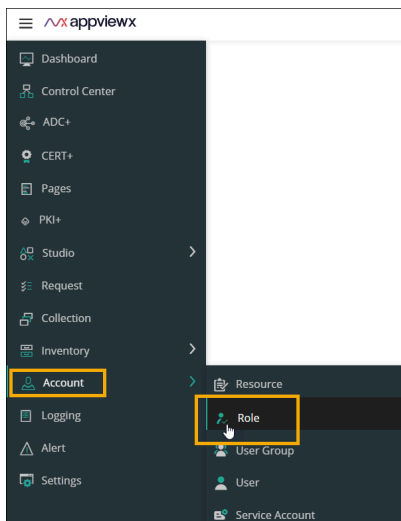
- From the top right corner of the screen, click **Enable**.
- In the **Confirmation** dialog box, click **Yes**.

The selected role is enabled.

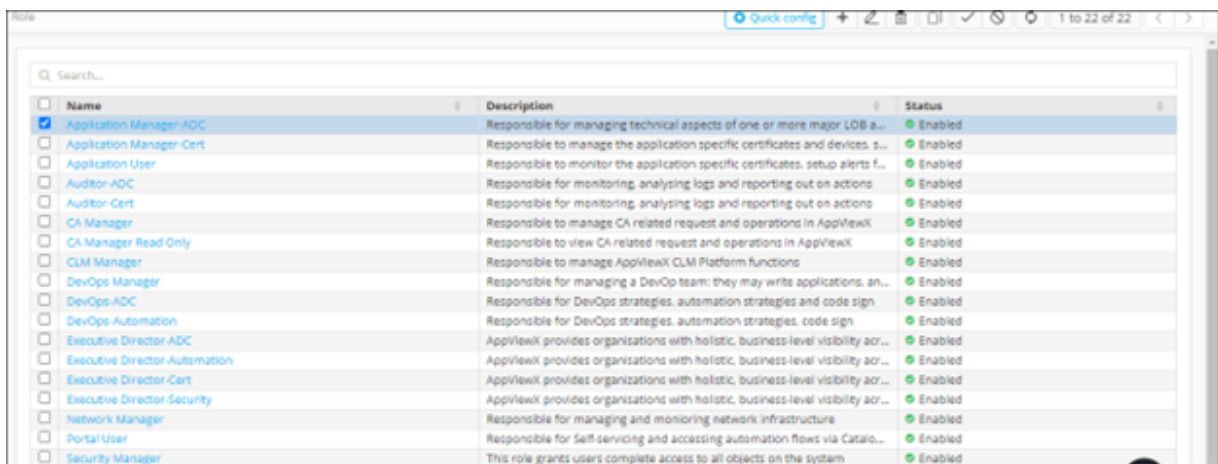
Disabling a Role

To disable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.



The **Role** page is displayed.



Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX.	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX.	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☐ DevOps Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled

3. For the (enabled) role you want to disable, select the corresponding check box.



4. From the top right corner of the screen, click .
5. In the **Confirmation** dialog box, click **Yes**.

The selected role is disabled.

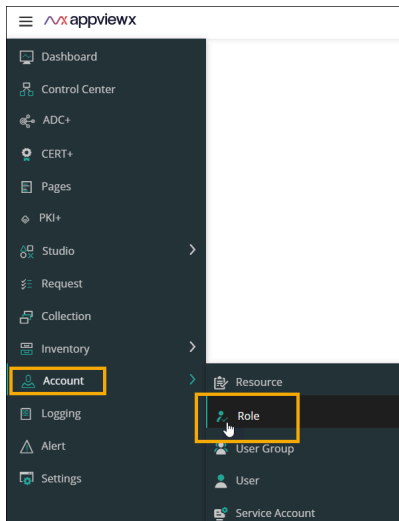
Deleting a Role



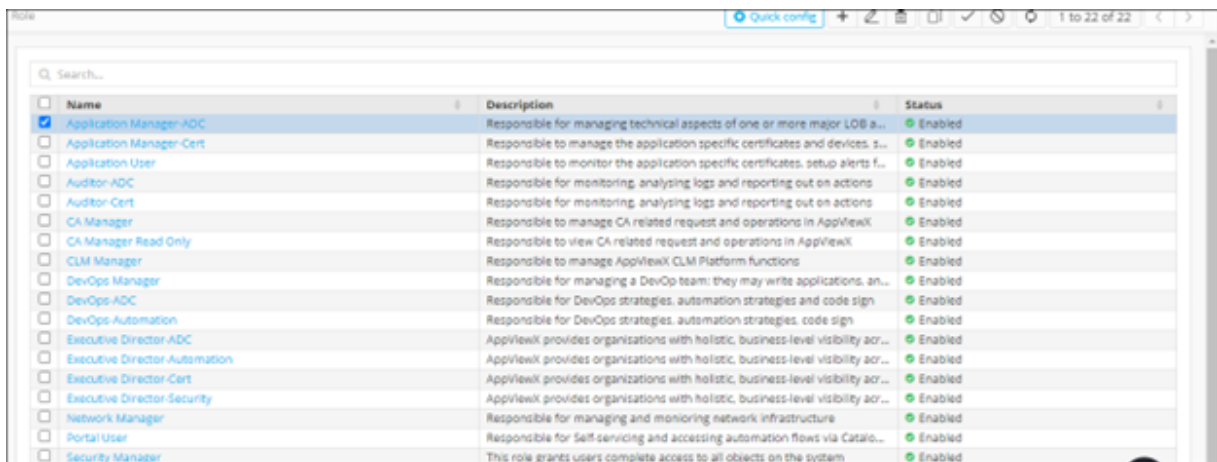
Note: A role that has active users belonging to it cannot be deleted.

To delete a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, select **Account > Role**.



3. The **Role** page is displayed.



Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices, s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign...	Enabled
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign...	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled

4. For the record you want to delete, select the corresponding check box.



5. From the top right corner of the screen, click

6. In the **Confirmation** dialog box, click **Yes**.

The selected role is deleted.

RBAC Quick Configuration

Simplified RBAC Configuration in AppViewX

To simplify existing RBAC Configuration in AppViewX for the Account Administrator, the Quick Config wizard flow option has been introduced in the existing Authentication, User groups, Roles and Resources. Using the Quick Config option, users should be able to perform all the following actions in the same wizard flow:

- Configure external authentication or single-sign-on for users to log in to AppViewX
- Add users groups into AppViewX by pulling specific user groups from AD into AppViewX based on specific patterns/keywords/codes and support Bulk Export/Import option to onboard user groups
- Pre-packaged roles for ADC, Cert, Security, and Automation modules to assign permissions to user groups
- Simplifying custom role creation by providing information help against each ACF explaining the significance of the functionality
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query or using a script and assigning permissions to user groups dynamically.
- [Authentication](#)
- [Resource](#)
- [Role](#)
- [User Group](#)

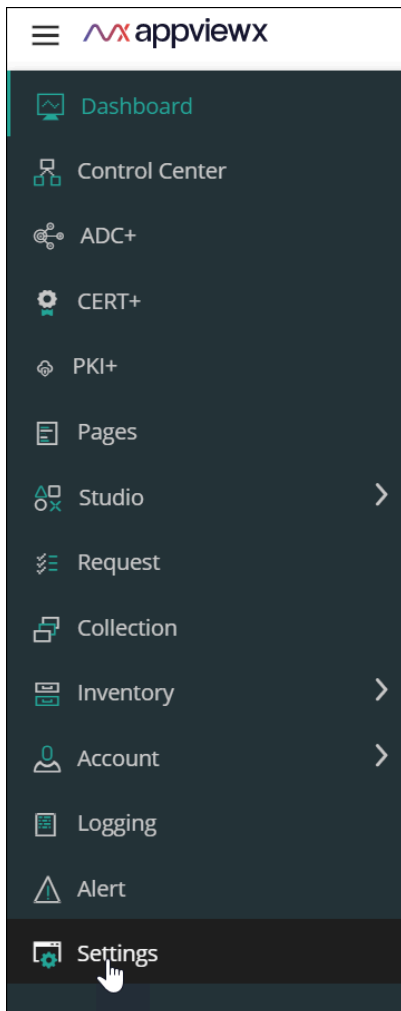
Authentication

- [Configure the Role-Based Access Control for LDAP](#)
- [Configuring Role-Based Access Control for TACACS](#)
- [Configuring Role-Based Access Control for RADIUS](#)
- [Configuring Single Sign On Settings with AppViewX](#)
- [Configuring Authentication Settings rbac quick config](#)

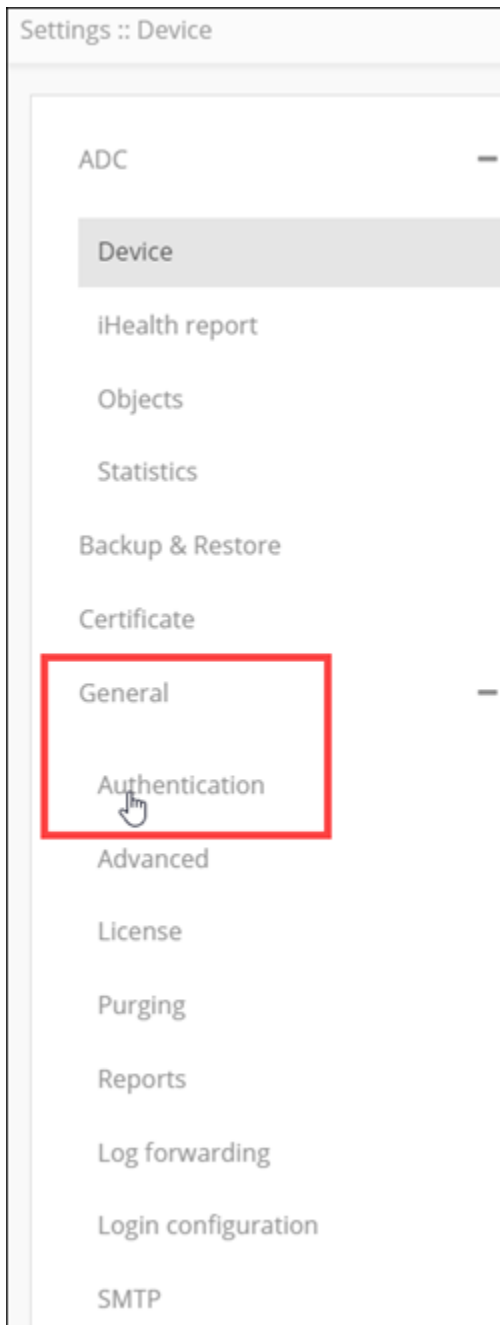
Configure the Role-Based Access Control for LDAP

To configure the RBAC settings for LDAP:

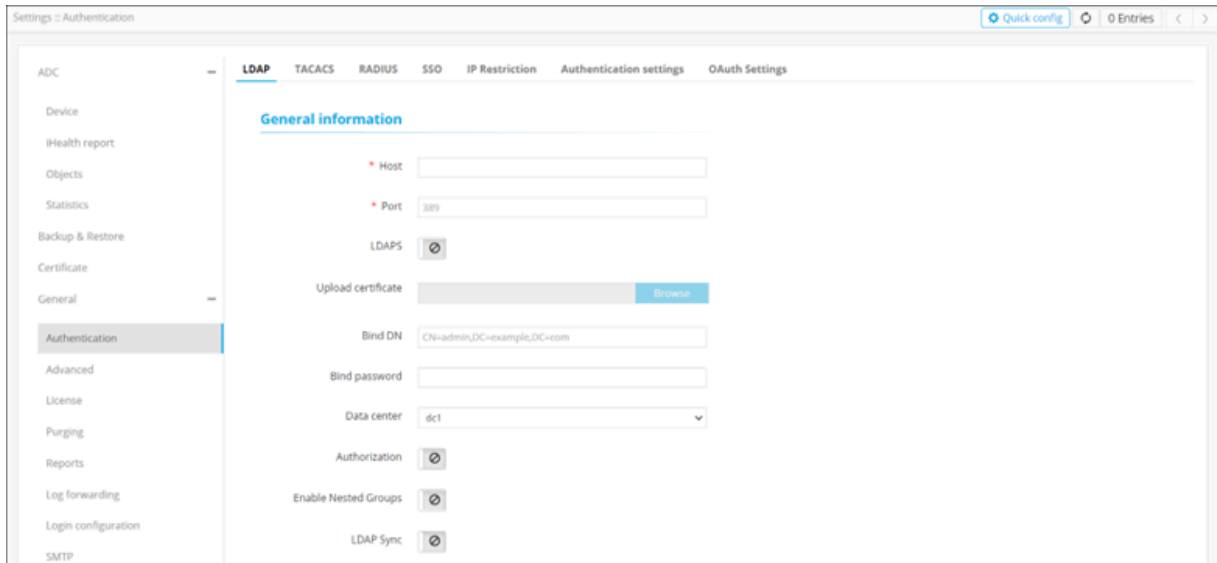
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



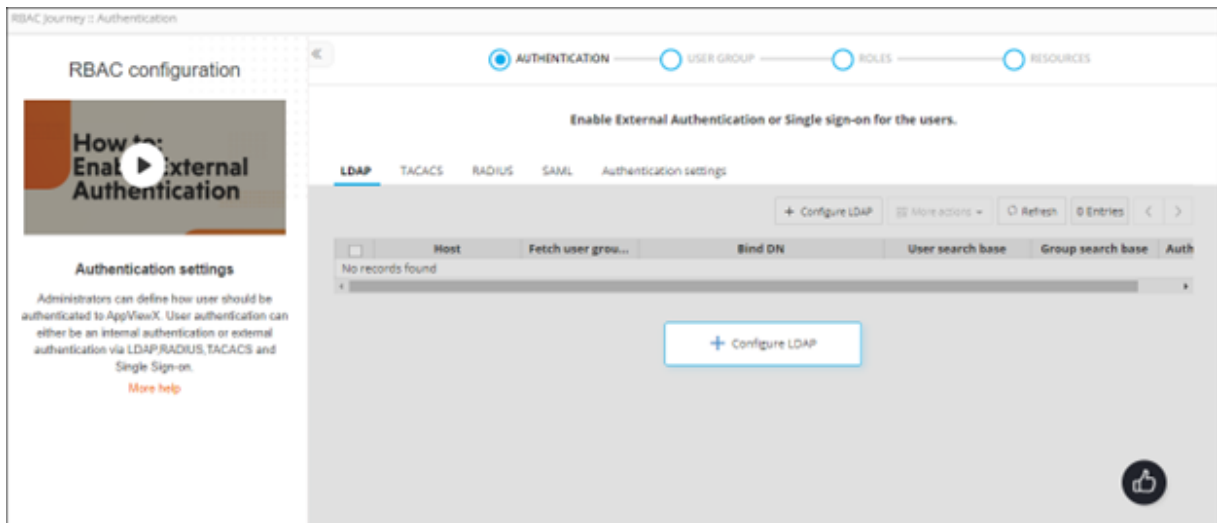
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



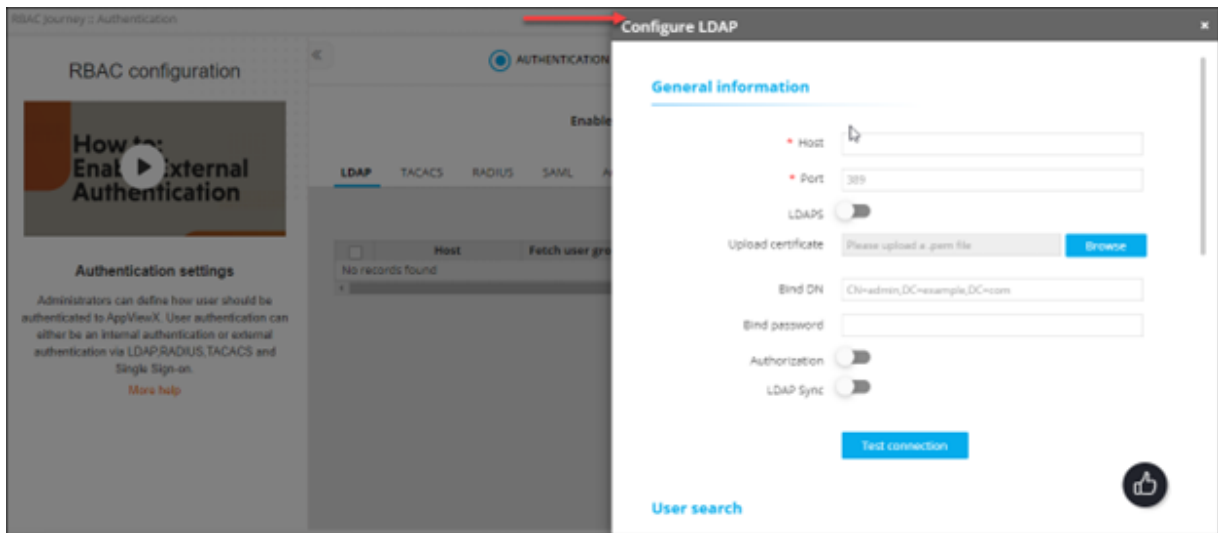
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



- From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



- On the **RBAC Journey :: Authentication** page, click **Configure LDAP**. The **Configure LDAP** action pane is displayed.



7. In the **General Information** section, enter the following details (sample values are shown in the image below the table):

Field	Description
*Host	Host name (domain name) of the LDAP server.
Port	Port number of the LDAP server.  Note: This value is entered based on the port number used in your deployment. By default, port number 389 is used for a LDAP configuration and port number 636 is used for a LDAPS configuration.
LDAP	The LDAPS protocol is used for secure communication between AppViewX and Active Directory/Open LDAP. To enable use of the LDAPS protocol authentication, instead of the LDAP protocol, turn on this toggle.
Upload certificate	 Note: This field is enabled only when the LDAPS is enabled. To upload a LDAP server certificate: - Click Browse Certificate. - Navigate to the location of the .pem certificate file.

Field	Description
	 Note: If the LDAP servers are load balanced with VIP, upload the root certificate of the LDAP server instead of the server certificate. c. Select the certificate to be uploaded and click Open. The selected certificate is uploaded.  Note: Only a single certificate can be uploaded for each server.
Bind DN	Username of the base authentication endpoint that will be used to connect to LDAP.
Bind Password	The password of the base authentication endpoint that will be used to connect to LDAP.
Authorization	To check user permissions at the time of authentication, select this check box. In addition to authentication, AppViewX also lets you perform user authorization against the LDAP server. To enable authorization along with authentication, select this check box.  Note: If Authorization is not enabled, AppViewX will only carry out LDAP authentication for the given user.
LDAP Sync	To enable the use of the SSH module in AppViewX for SSH key discovery use case, turn on this toggle.
All * marked fields are mandatory.	

General information

* Host

* Port

LDAPS

☐

Upload certificate

Please upload a .pem file

Bind DN

Bind password

Authorization

☒

LDAP Sync

☐

8. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click **Test Connection**.



Note: You can test the connection of LDAPS only when you save all of the configuration details. Bind DN and Bind password details cannot be validated through a test connection.

9. The **User Search** section collects information to validate a user's presence in the Active Directory. In the **User Search** section, enter the following details(sample values are shown in the image below the table):

Field	Description
*User search base	Base directory where the user is present.
*Search filter	Criteria for searching for the user from the search base.
*User return attribute	User information to be retrieved from the search base.

Field	Description
	 Note: This field is enabled only when the Authorization toggle (in the General Information section) is turned on.  Note: You can specify only User return attribute.
All * marked fields are mandatory.	

User search

* User search base

* Search filter

* User return attribute

112 remaining

Test query



- After entering the above details, to test if the user is present in the Active Directory, click **Test query**.
- In the **User search result** action pane, enter the **Test username** and click **Test**.



The image shows a 'User search result' dialog box. At the top, it has a title bar with the text 'User search result' and a close button. Below the title bar, there is a label '* Test username' followed by a text input field containing 'pmuser1@testavx.com'. To the right of the input field is an information icon. Below the input field is a blue 'Test' button. The main area of the dialog is a large black rectangle, and in the bottom right corner of this rectangle is a white thumbs-up icon.



Note: You are allowed to check the query response for User search and Group search only when the connection is valid.

12. To test which user group the user belongs to, in the **Group search** section, enter the following details:



Note: This section is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on.

Field	Description
Group search base	Base directory where the user group is present.
Search filter	Criteria to search the user group from the search base.
Group return attribute	User group information to be retrieved from the search base.



Note: You are allowed to check the query response for User search and Group search only when the connection is valid.



Note: Group search can be performed only if the customer's LDAP is of type Open LDAP. Microsoft Active Directory does not need group search configuration. For Open LDAP, group search needs to be configured mandatorily. The User return attribute in the User search section does not return the group membership details.



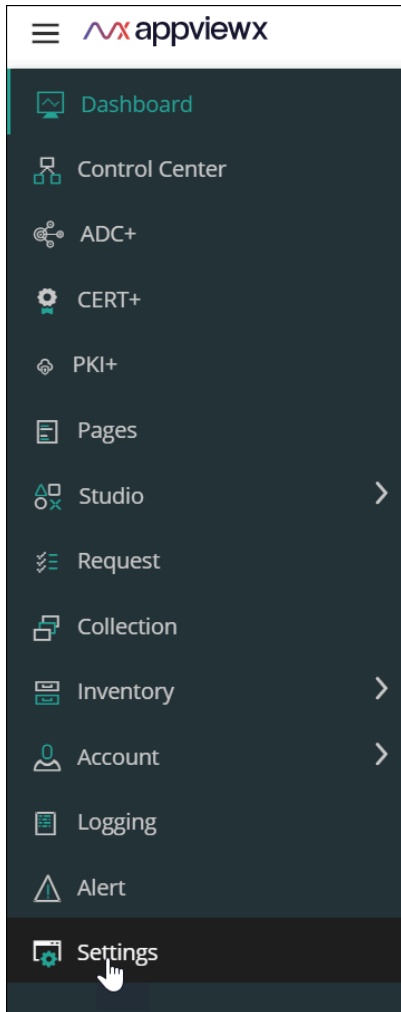
Note: In the case of multiple LDAP servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- [Deleting a LDAP Configuration](#)

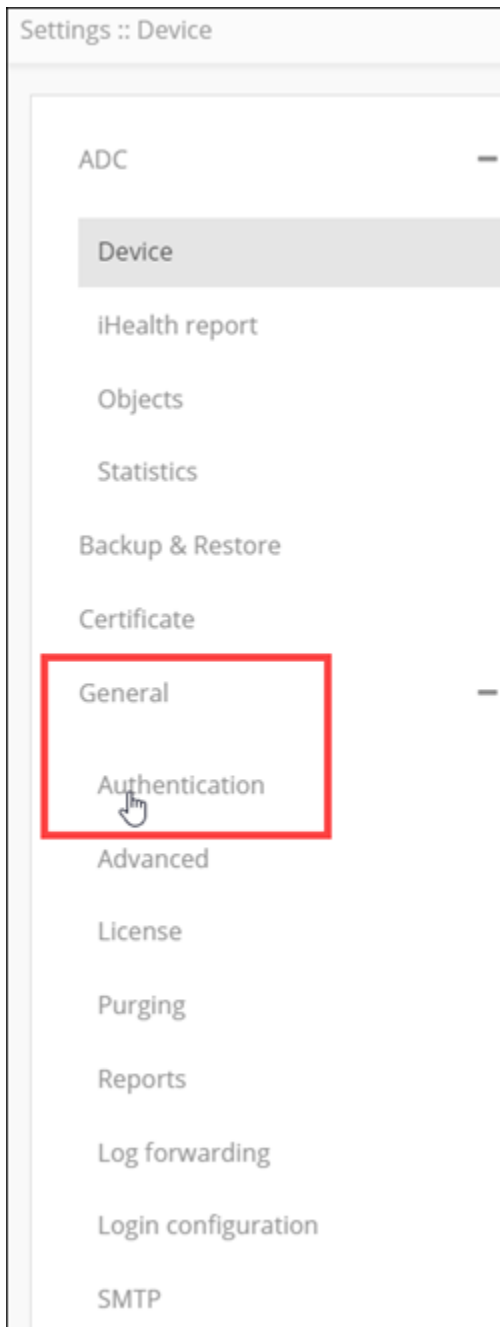
Deleting a LDAP Configuration

To delete a LDAP configuration:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



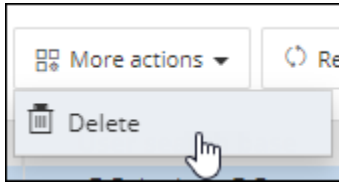
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

5. From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.

6. From the table of LDAP configurations, to delete a LDAP configuration, select the check box corresponding to that entry.

☒	Host	Fetch user grou...	Bind DN	User search base	Group search base	Auth
☒	ldaps://gs-ldap-pe1.la...	Fetch	CN=Administrator,CN=Users,DC=testavx,...	DC=testavx,DC=com	DC=testavx,DC=com	ti

7. From the **More actions** drop-down menu, click **Delete**.



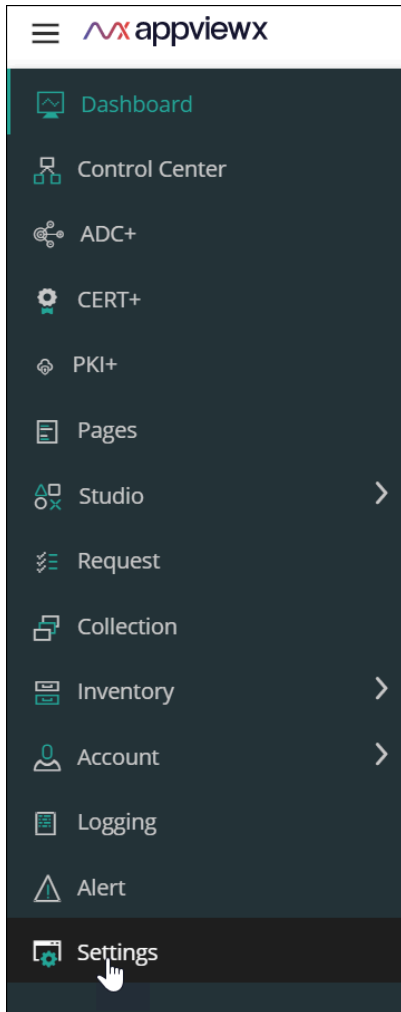
8. In the **Confirmation** dialog box, click **Delete**.

The selected configuration is deleted.

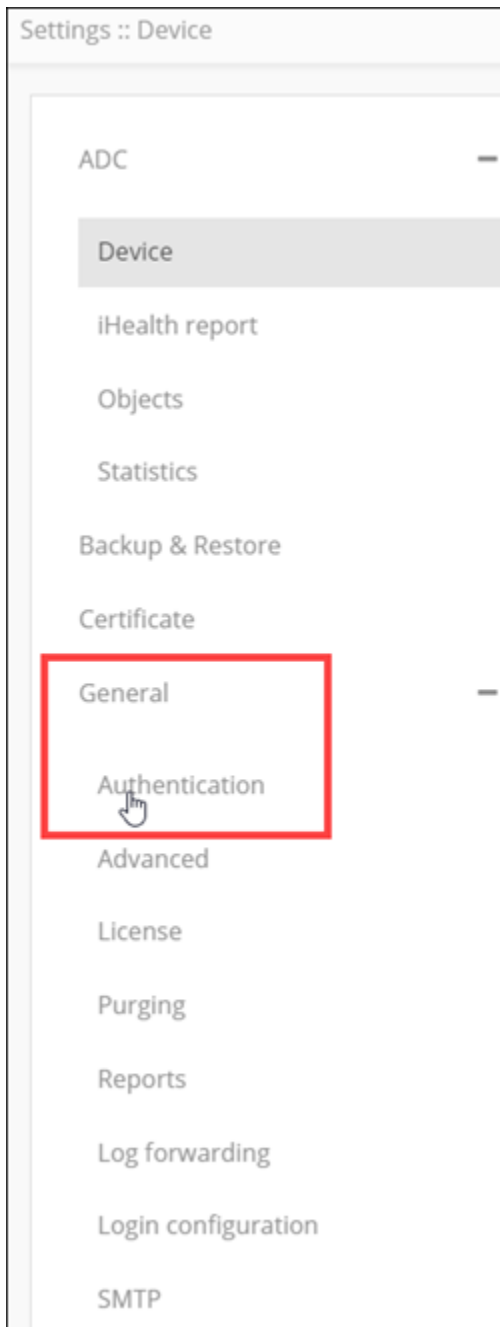
Configuring Role-Based Access Control for TACACS

To configure RBAC for TACACS authentication:

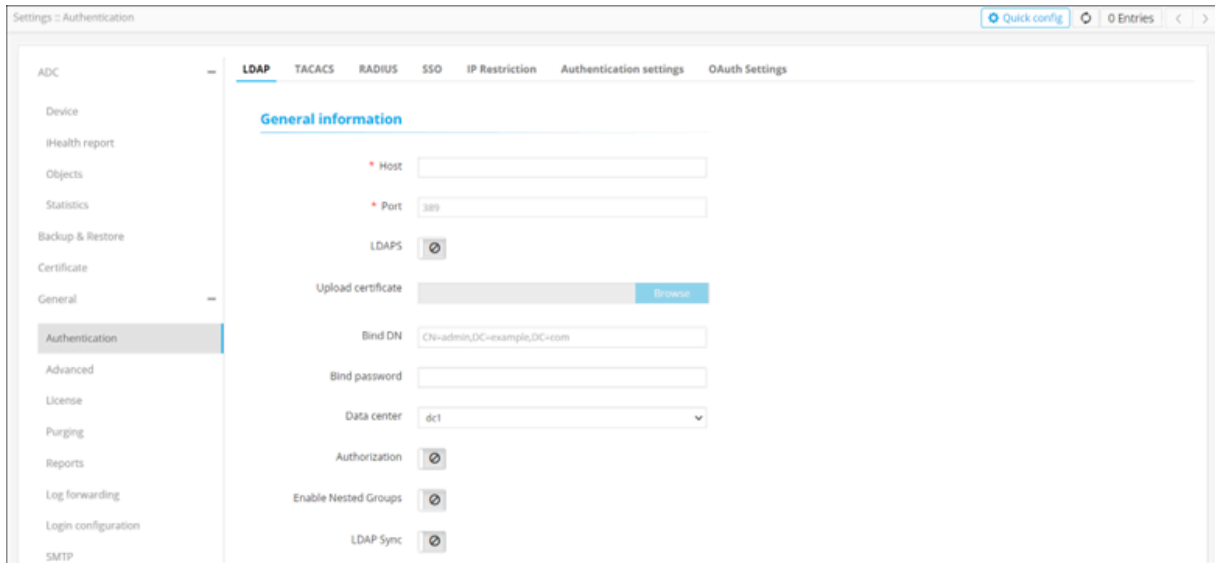
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



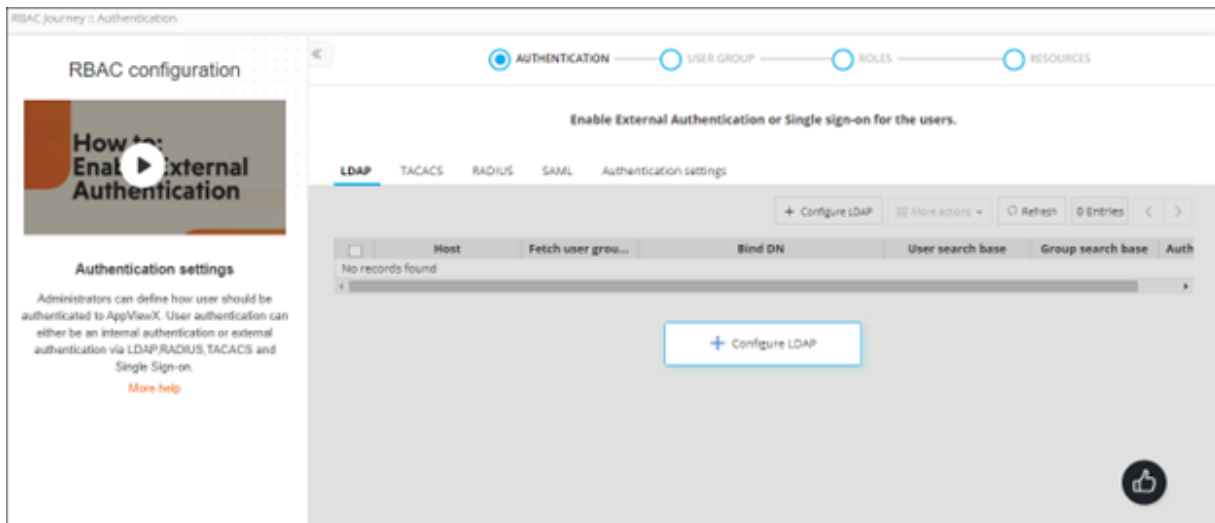
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



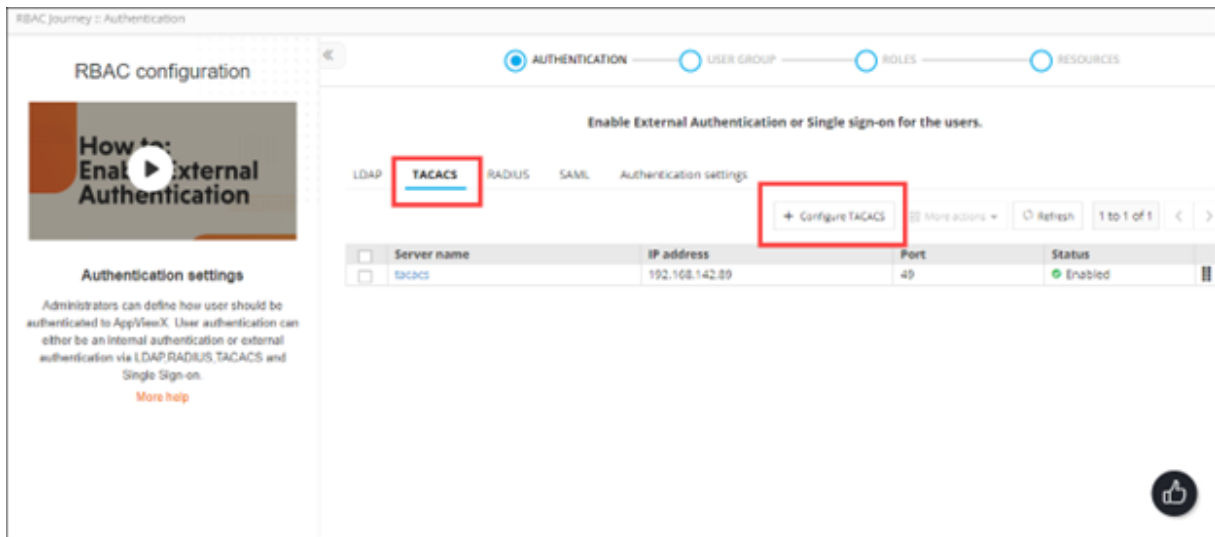
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



- From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.



- On the **RBAC Journey :: Authentication** page, click the **TACACS** tab and click **Configure TACACS**.



The **Configure TACACS** action pane is displayed.

The 'Configure TACACS' action pane is displayed. It has a title bar with a close button (X). The form contains the following fields, each with a red asterisk indicating it is required:

- Server name
- IP address
- Port
- Secret key
- Service
- Protocol
- Authorization attribute name

There is a blue 'Test connection' button between the 'Port' and 'Secret key' fields. At the bottom, there are 'Add' and 'Cancel' buttons. A thumbs-up icon is visible in the bottom right corner.

7. Enter the field information as shown in the table below:

Field	Description
*Server name	Name of the TACACS server.
*IP address	IP address of the TACACS server.
*Port	Port number of the TACACS server
All * marked fields are mandatory.	

8. To test the connectivity between AppViewX and the IP address mentioned above, click **Test connection**.

9. Enter the field information as shown in the table below::

Field	Description
*Secret key	A unique key for authentication between the AppViewX server and the TACACS server.
*Service	Name of the service used by the user requested to be authorized. Specifying the service name is mandatory because it enables the TACACS + server to behave according to the type of each authorization request. Commonly, the Point-to-Point Protocol (PPP) is used for authorization checks.
*Protocol	The protocol associated with the value specified in Service Name, which is a subset of the associated service being used for client authorization or system accounting Commonly, the Internet Protocol (IP) is used as the modifier with PPP to indicate the protocol layer for authorization check.
*Authorization Attribute Name	Attribute that will be returned from the TACACS server to authenticate and authorize the connection between the AppViewX server and the TACACS server.
All * marked fields are mandatory.	

10. To save the TACACS authentication settings, click **Add** and to reconfigure the settings, click **Reset**. The TACACS authentication settings thus configured are saved and displayed in the table as shown in the image below:

☐	Server name	IP address	Port	Status	
☐	tacacs	192.168.142.89	49	Enabled	



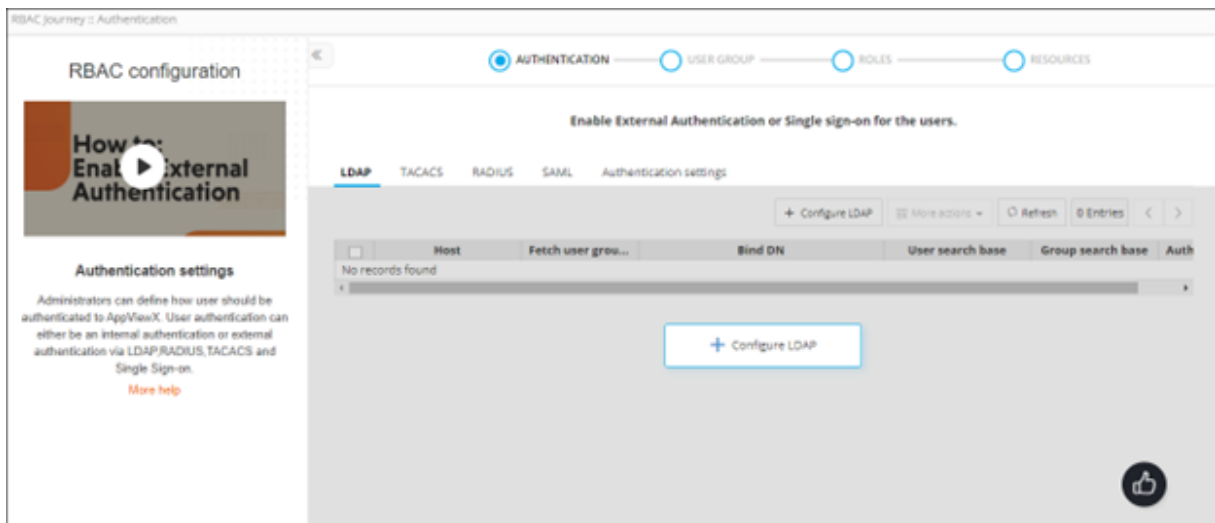
Note: In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- Enabling a TACACS Configuration
- Disabling a TACACS Configuration
- Deleting a TACACS Configuration

Enabling a TACACS Configuration

To enable a TACACS configuration:

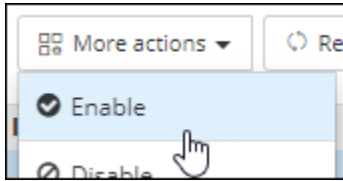
1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



3. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab.
4. From the table of TACACS configurations, for the configuration you want to enable, select the check box corresponding to that entry.

☒	Server name	IP address	Port	Status	
☒	tacacs	192.168.142.89	49	Disabled	

5. From the **More actions** drop-down menu, click **Enable**.



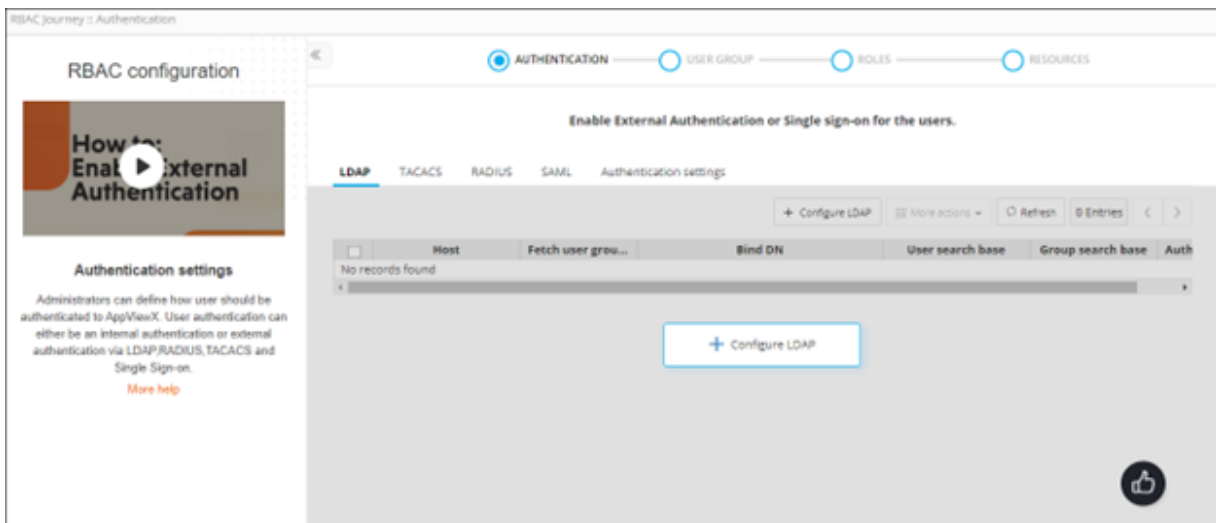
6. In the **Confirmation** message dialog box, click **Proceed**.

The selected configuration is enabled.

Disabling a TACACS Configuration

To disable a TACACS configuration:

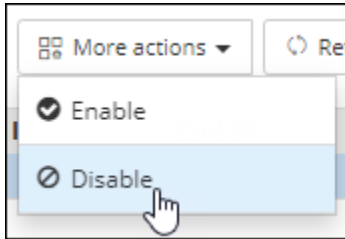
1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.



3. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab.
4. From the table of TACACS configurations, for the configuration you want to disable, select the check box corresponding to that entry.

☒	Server name	IP address	Port	Status	
☒	tacacs	192.168.142.89	49	Enabled	

5. From the **More actions** drop-down menu, click **Disable**.

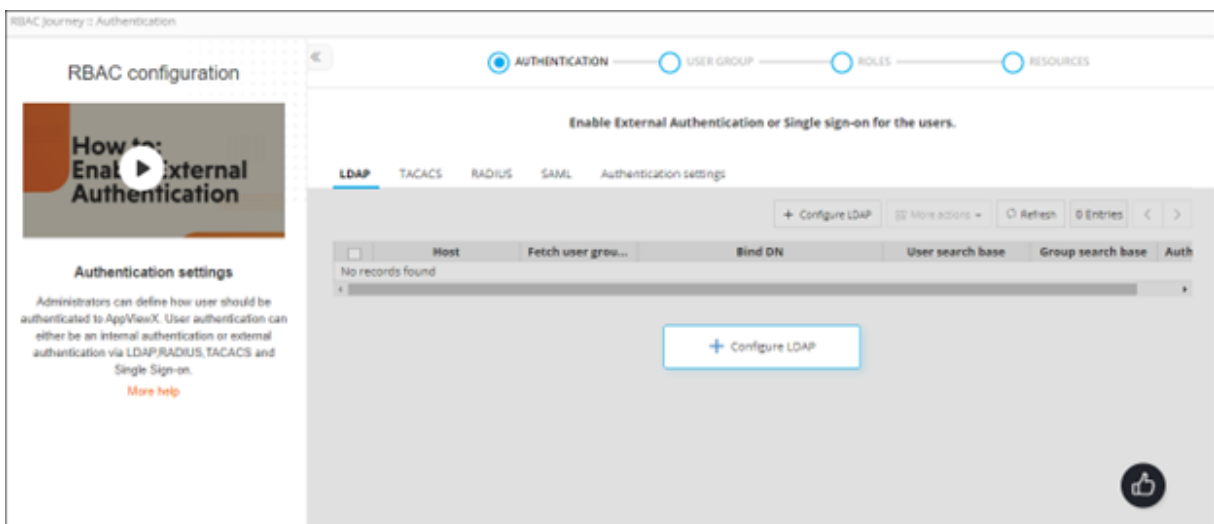


6. In the **Confirmation** message dialog box, click **Proceed**.
The selected configuration is disabled.

Deleting a TACACS Configuration

To delete a TACACS configuration:

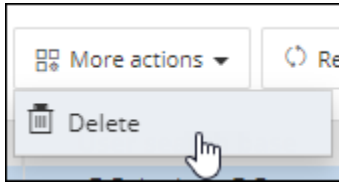
1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.



3. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab.
4. From the table of TACACS configurations, for the configuration you want to delete, select the check box corresponding to that entry.

☒	Server name	IP address	Port	Status	
☒	tacacs	192.168.142.89	49	Enabled	

5. From the **More actions** drop-down menu, click **Delete**.



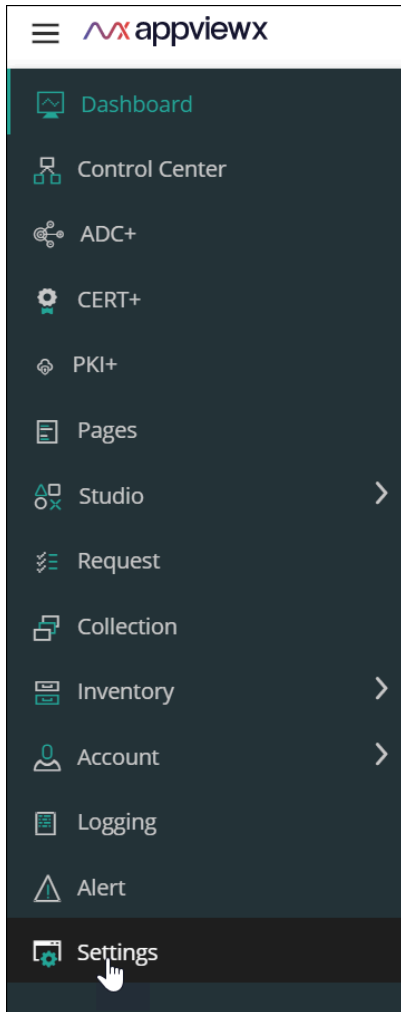
6. In the **Confirmation** message dialog box, click **Proceed**.

The selected configuration is deleted.

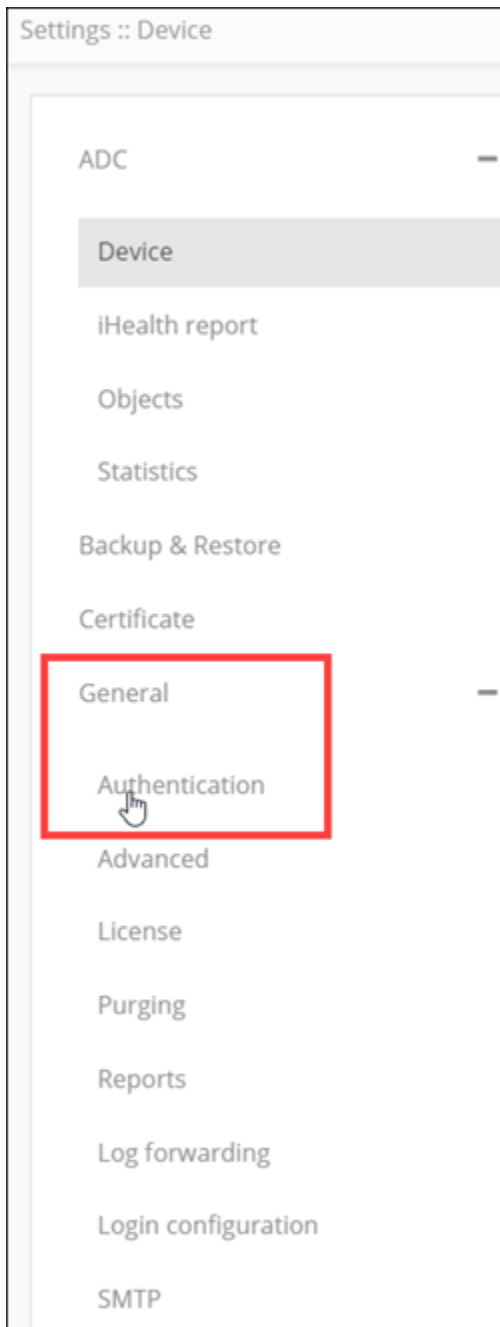
Configuring Role-Based Access Control for RADIUS

To configure RBAC for RADIUS authentication:

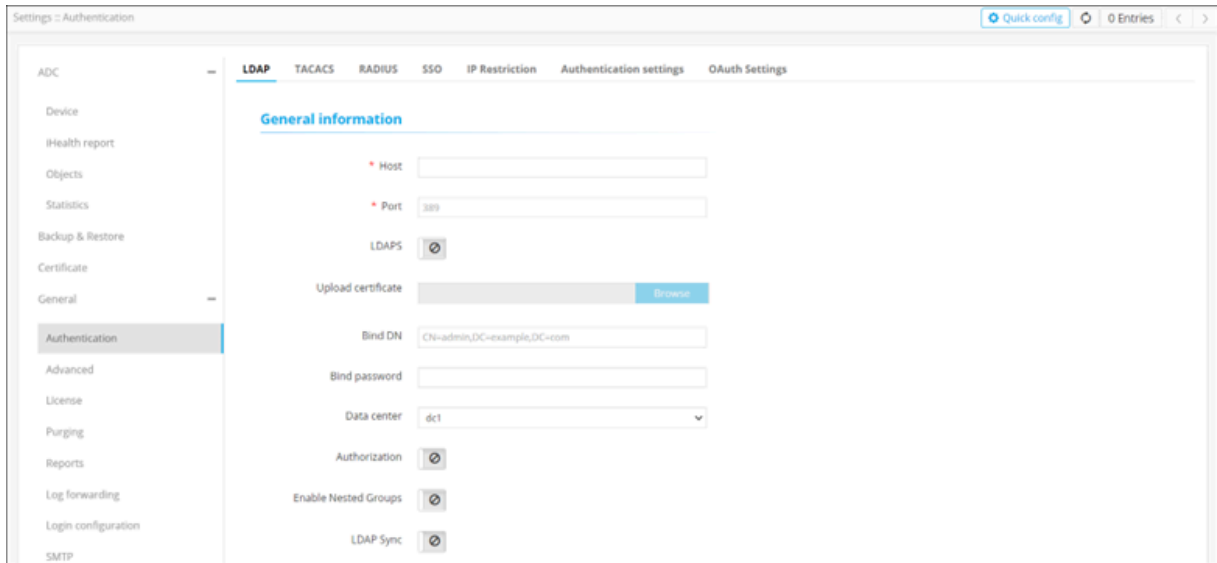
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



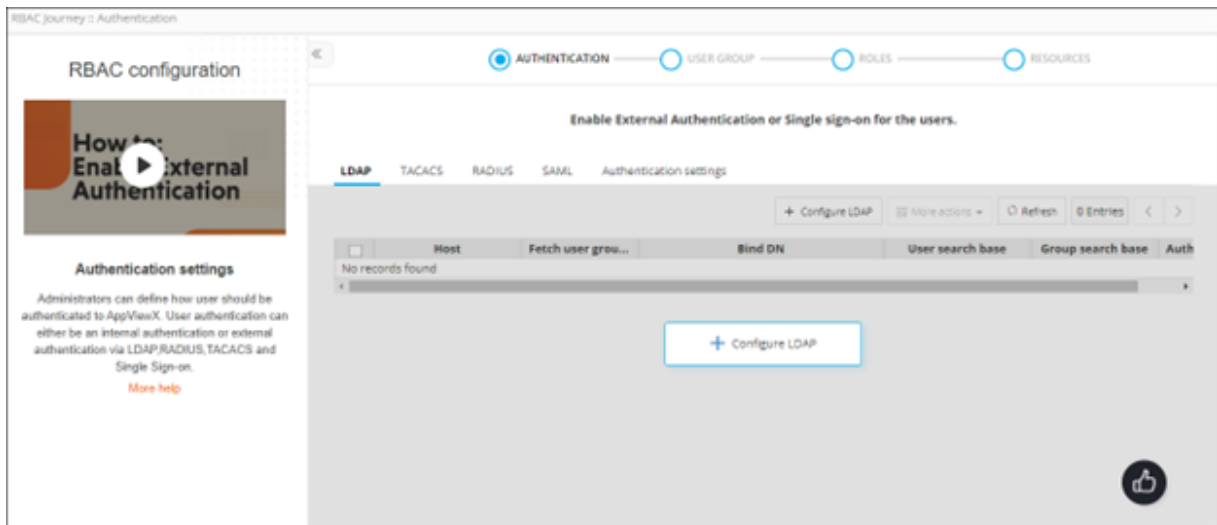
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



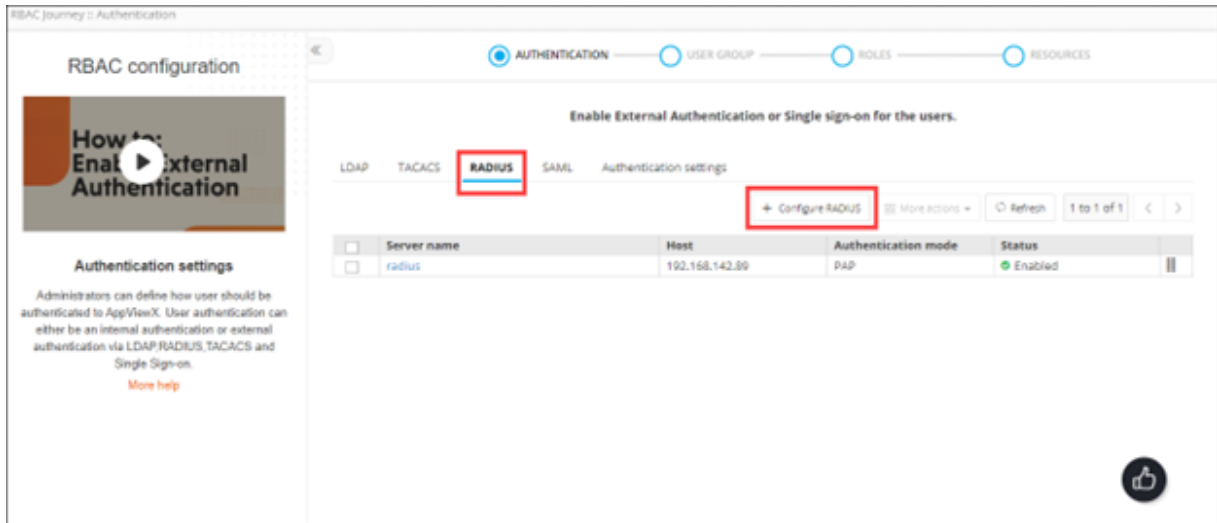
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



- From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



- On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab and click **Configure RADIUS**.



The Configure RADIUS action is displayed.

The 'Configure RADIUS' dialog box contains the following fields and options:

- Server name**: Text input field.
- Host**: Text input field.
- Shared secret**: Text input field.
- Authentication port**: Text input field.
- Acceptance port**: Text input field.
- Authentication mode**: Radio buttons for PAP/ASCII (selected), CHAP, MS-CHAPv2, and EAP-MD5.
- Authorization**: Toggle switch (turned on).
- Authorization via**: Radio buttons for Radius (selected) and LDAP.
- Vendor ID**: Text input field.
- Vendor type**: Text input field.

A thumbs-up icon is visible in the bottom right corner of the dialog box.

7. Enter the field information as described in the following table:

Field	Description
*Server Name	Name of the RADIUS server.
*Host	The IP address of the RADIUS server.
*Shared secret	A unique key for authentication between the AppViewX server and the RADIUS server.
*Authentication port	Port number that AppViewX will use for authentication.  Note: The default authentication port number is 1812. Please check with your sysadmin if your organization uses a different port number.
*Acceptance port	Port number that AppViewX will use to accept a response from the RADIUS server.  Note: The default acceptance port number is 1813. Please check with your sysadmin if your organization uses a different port number.
*Authentication mode	Select one of the following authentication modes: • PAP/ASCII • CHAP • MS-CHAPv2 • EAP-MD5  Note: Ensure that the selected authentication mode is also confirmed in the RADIUS server settings.
Authorization via	Select from one of the following authorization modes: • RADIUS • LDAP  Note: This field is enabled only when the Authorization toggle is turned on.
*Vendor ID	Enter the vendor ID.

Field	Description
	 Note: This field is enabled only whrn the the Authorization toggle is turned on and authorization is done via the RADIUS server.  Note: AppViewX does not have a unique vendor ID. We use a free vendor ID: 500. Ensure that this is configured as part of the RADIUS server settings.
*Vendor type	Enter the vendor type.  Note: This field is enabled only whrn the the Authorization toggle is turned on and authorization is done via the RADIUS server.  Note: AppViewX does not have a unique vendor type. We use a free vendor ID: 200. Ensure that this is configured as part of the RADIUS server settings.
*LDAP	From the dropdown menu, select the LDAP server to be used for the authorization.  Note: This field is enabled only whrn the the Authorization toggle is turned on and authorization is done via the LDAP server.
All * marked fields are mandatory.	

8. To save the RADIUS authentication settings entered above, click **Add** or to reconfigure the settings, click **Reset**.

The RADIUS authentication settings thus configured are saved and displayed in the table as shown in the image given below:

☐	Server name	Host	Authentication mode	Status	
☐	radius	192.168.142.89	PAP	Enabled	



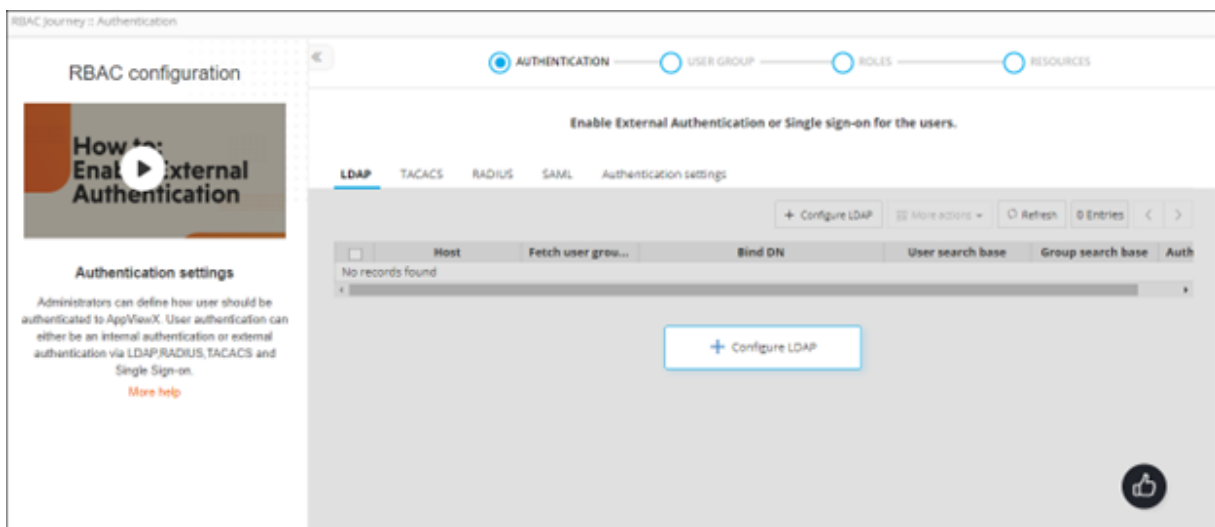
Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- Enabling a RADIUS Configuration
- Disabling a RADIUS Configuration
- Deleting a RADIUS Configuration

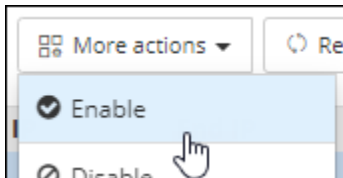
Enabling a RADIUS Configuration

To enable a RADIUS configuration:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



3. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab.
4. From the table of RADIUS configurations, for the configuration you want to enable, select the check box corresponding to that entry.
5. From the **More actions** drop-down menu, click **Enable**.

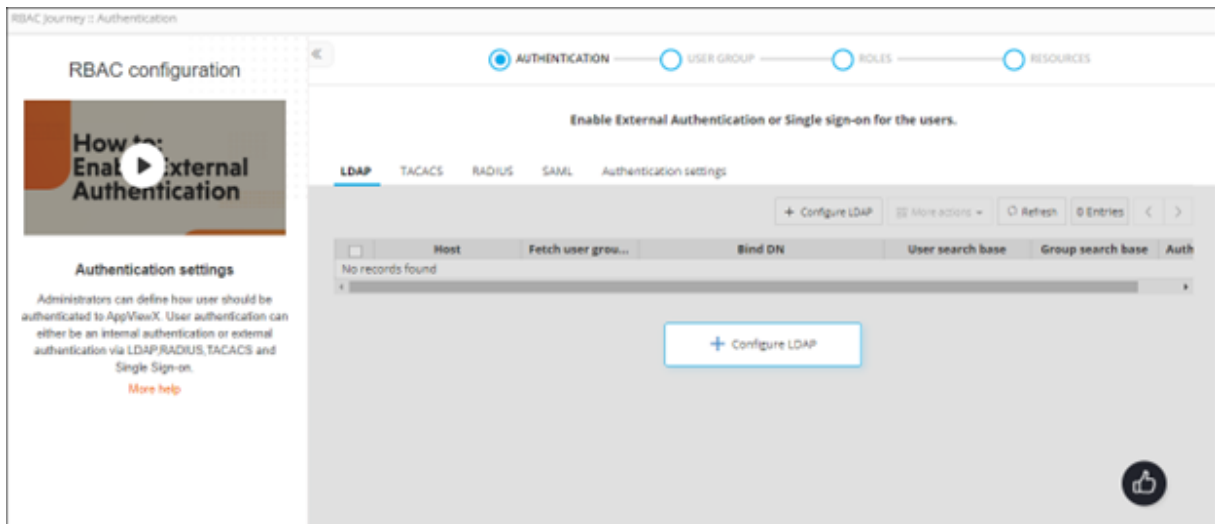


6. In the **Confirmation** message dialog box, click **Proceed**. The selected configuration is enabled.

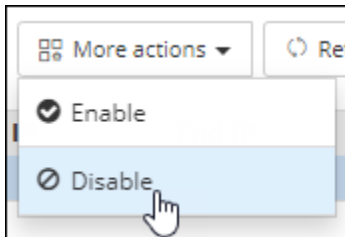
Disabling a RADIUS Configuration

To disable a RADIUS configuration:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



3. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab.
4. From the table of RADIUS configurations, for the configuration you want to disable, select the check box corresponding to that entry.
5. From the **More actions** drop-down menu, click **Disable**.

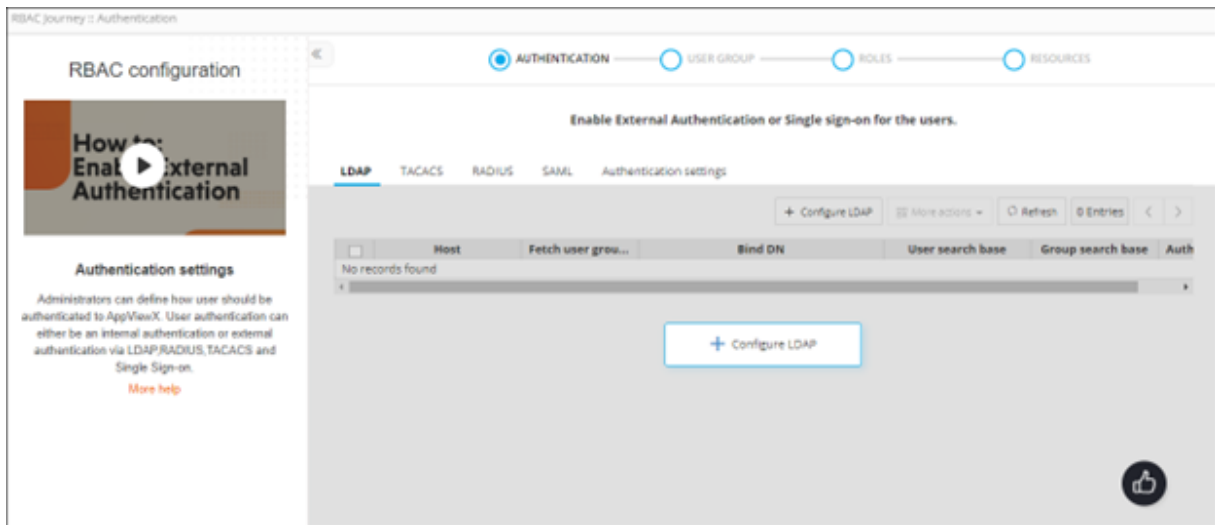


6. In the **Confirmation** message dialog box, click **Proceed**. The selected configuration is disabled.

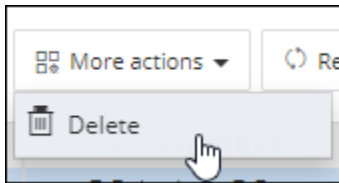
Deleting a RADIUS Configuration

To delete a RADIUS configuration:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



3. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab.
4. From the table of RADIUS configurations, for the configuration you want to delete, select the check box corresponding to that entry.
5. From the **More actions** drop-down menu, click **Delete**.

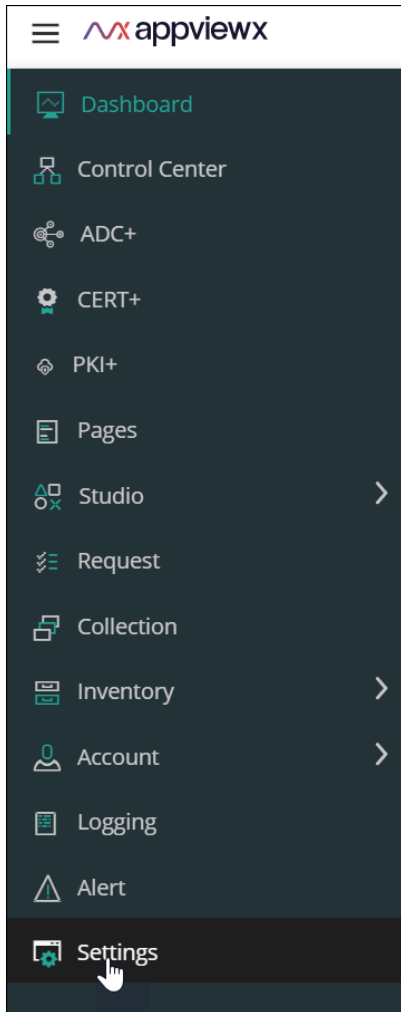


6. In the **Confirmation** message dialog box, click **Proceed**. The selected configuration is deleted.

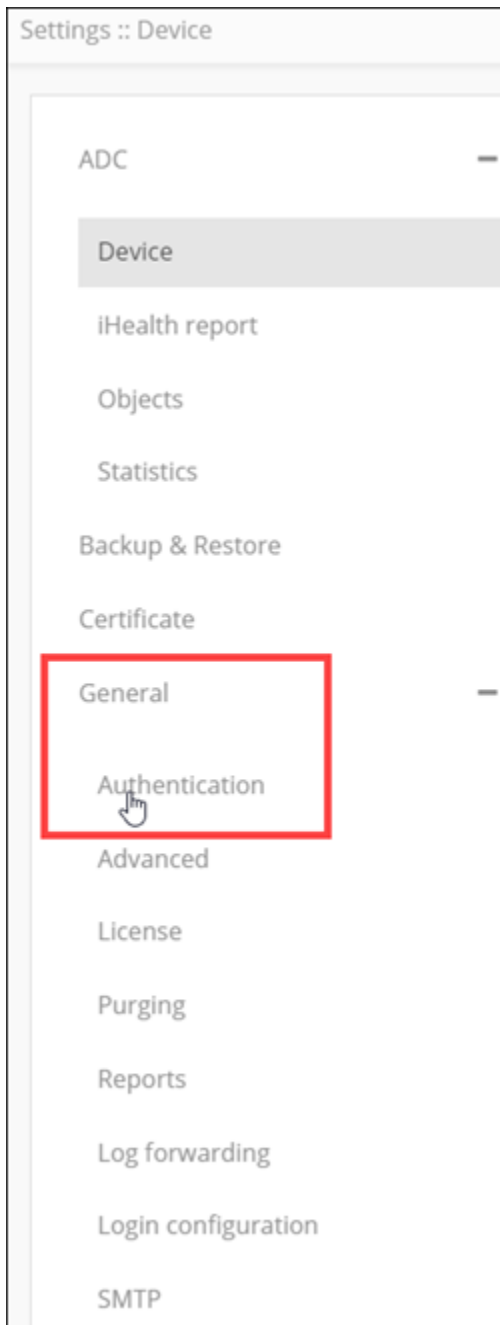
Configuring Single Sign On Settings with AppViewX

To configure single sign on settings with AppViewX:

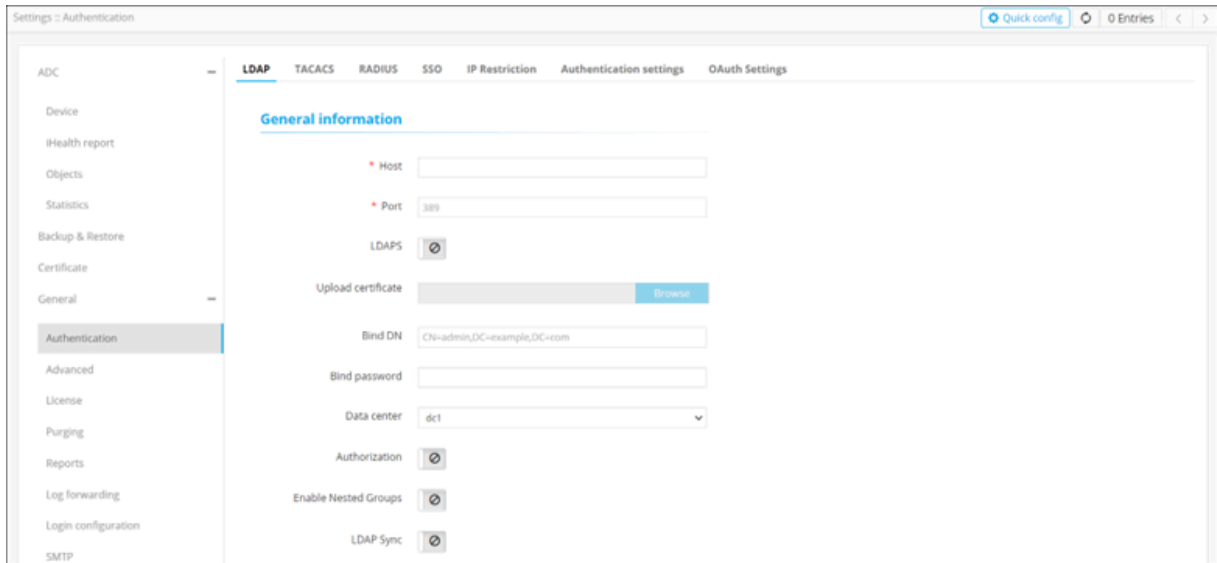
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



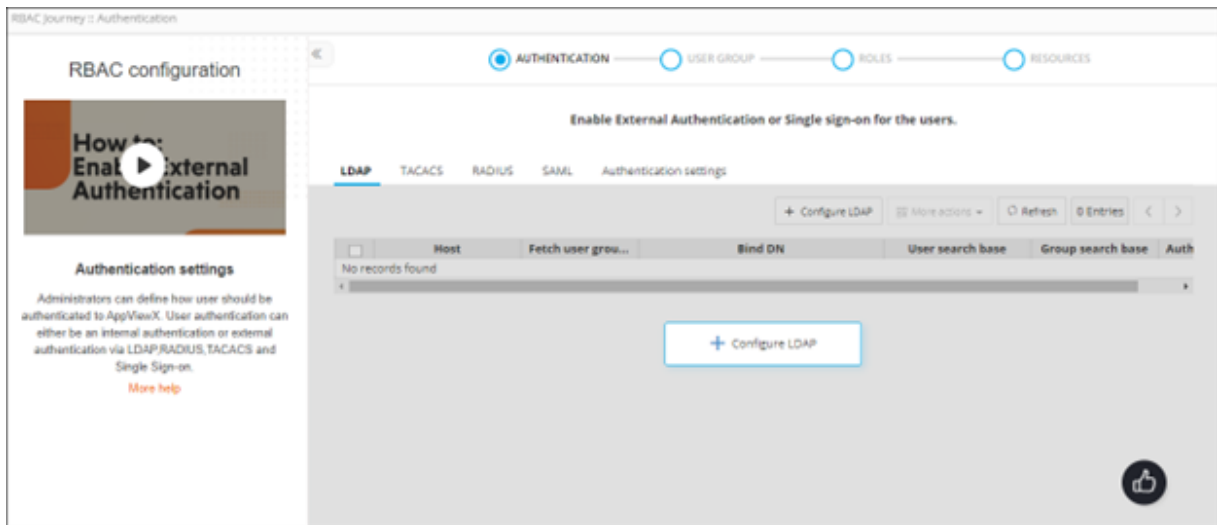
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



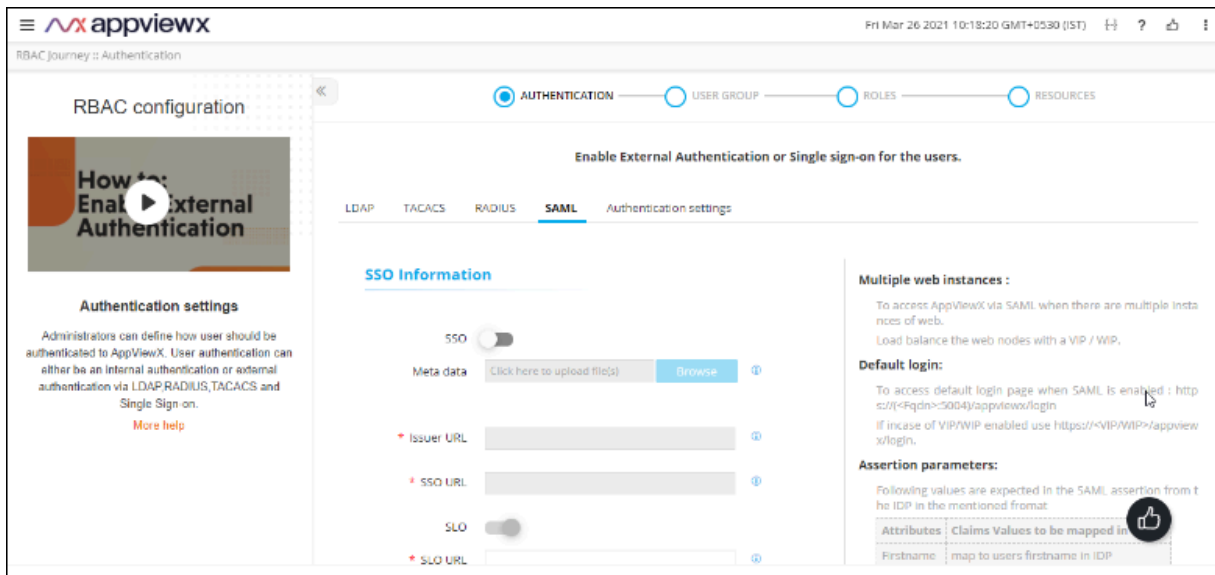
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



- From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.



- On the **RBAC Journey :: Authentication** page, click the **SAML** tab.



7. In the **SSO Information** section, enter the following details:

Field	Description
SSO	To use SAML authentication for Single Sign On, turn on the SSO toggle. The Config Information section is displayed with the field information auto-populated as shown below: Config Information Host: localhost:5004 Entity ID: localhost:5004/appviewx/ Service URL: localhost:5004/appviewx/ssoLogin SLO URL: localhost:5004/appviewx/logout
Metadata	To import an identity provider (IdP): - Click Browse. - Navigate to the location where the XML metadata file is stored. - To upload the file, click Open.

Field	Description
	 Note: You can also copy and paste the metadata information from the XML file into the metadata contents text boxes in the Config Information section.
*Issuer URL	Entity ID of the IdP.  Note: This field is enabled only when the SSO toggle in the SSO Information section is turned on.
*SSO URL	For AppViewX to send the authentication request, enter the URL of the protected endpoint provided by your IdP.  Note: This field is enabled only when the SSO toggle in the SSO Information section is turned on.
SLO	To enable single log out, turn on the SLO toggle. This will log out the user from AppViewX and the IdP.
*SLO URL	URL of the IdP protocol endpoint.  Note: This field is enabled only when the SSO toggle in the SSO Information section is turned on.  Note: This field is mandatory only when the SLO toggle in the SAML details section is turned on.
*Upload certificate	To upload a certificate: a. Click Browse Certificate . b. Navigate to the location of the .pem certificate file. c. Select the certificate file to be uploaded and click Open .The selected certificate is uploaded.  Note: A certificate is to be uploaded only when the certificate of the IDP is not available as a part of the metadata.

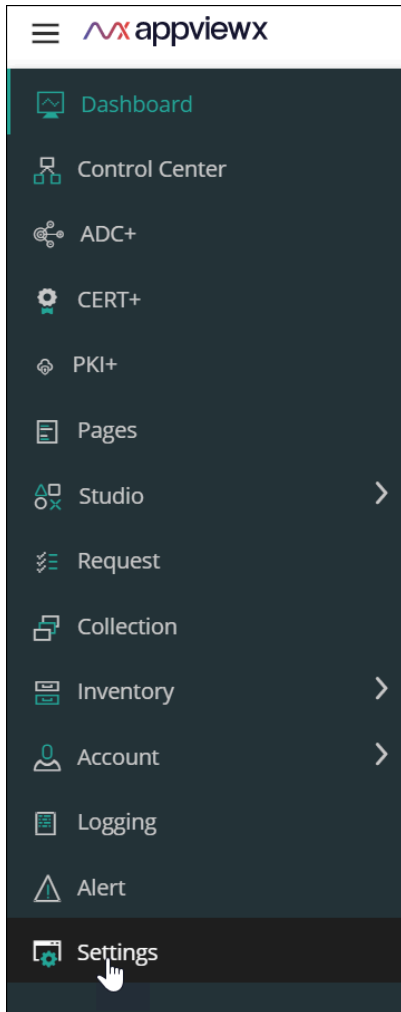
Field	Description
	 Note: This field is enabled only when the SSO toggle in the SSO Information section is turned on.
Local authorization	To enable SAML only authentication in IdP and for authorization to be carried out in AppViewX, enable this toggle key.  Note: Authorization can be done by assigning user groups manually to the user or enabling birthright role.
All * marked fields are mandatory.	

8. To save the SAML authentication settings, click **Save** or to cancel the authentication settings, click **Cancel**.

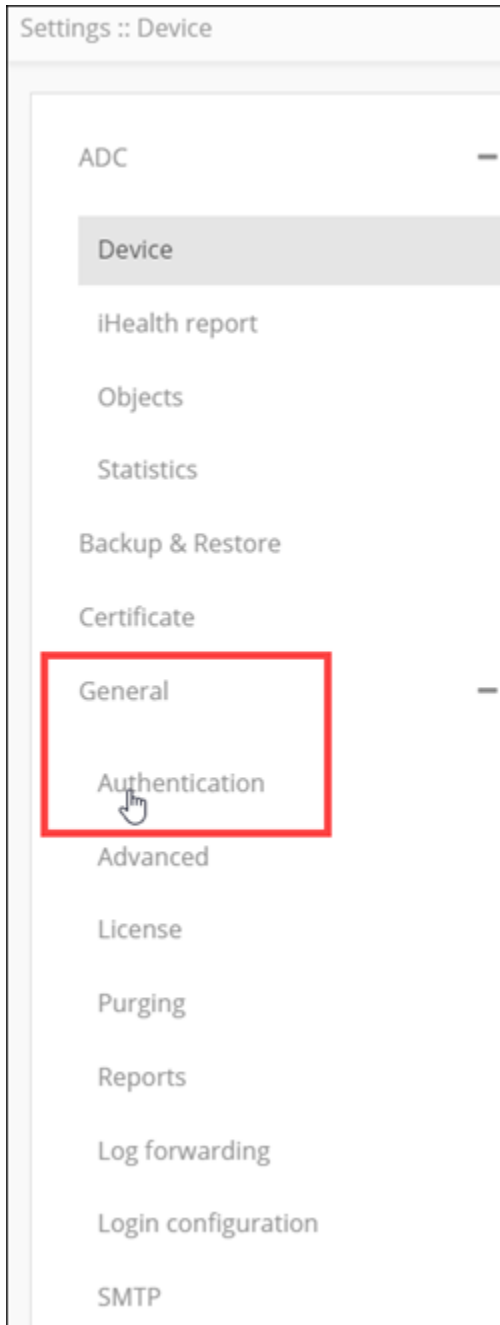
Configuring Authentication Settings rbac quick config

To configure the authentication settings:

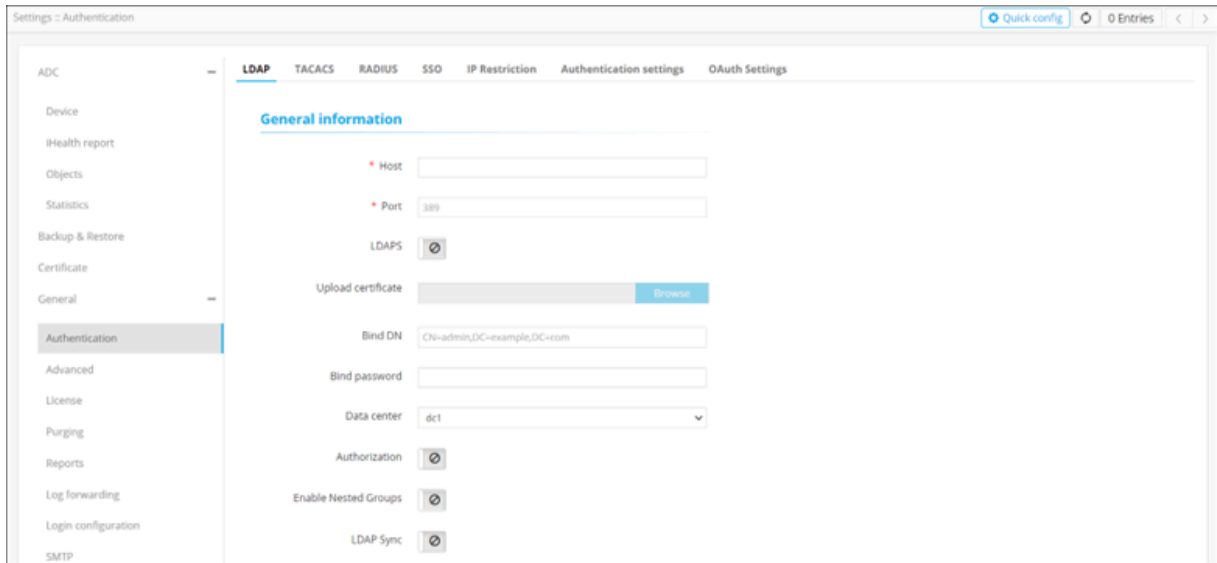
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



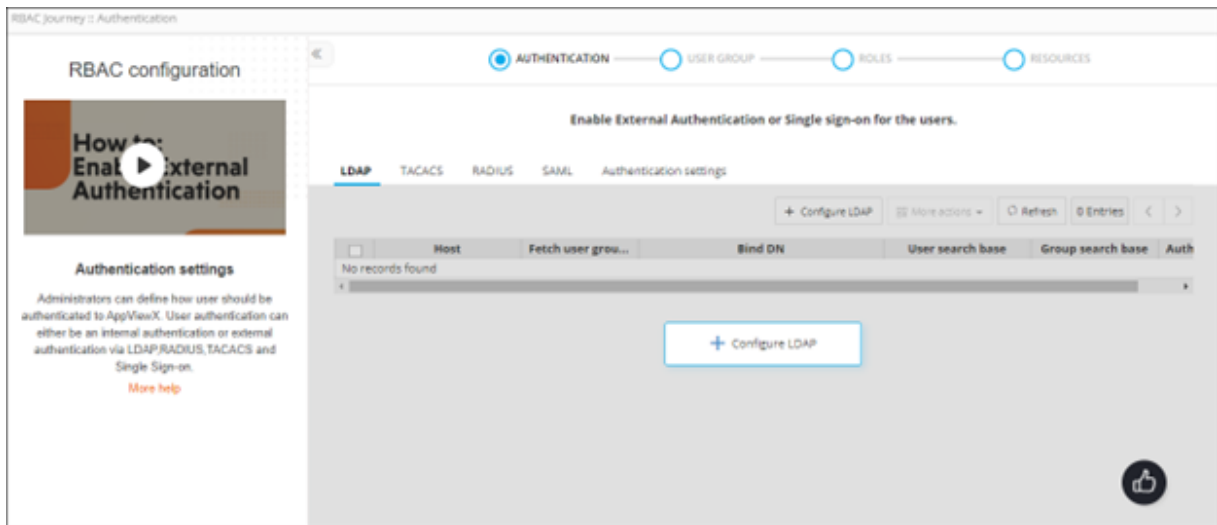
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



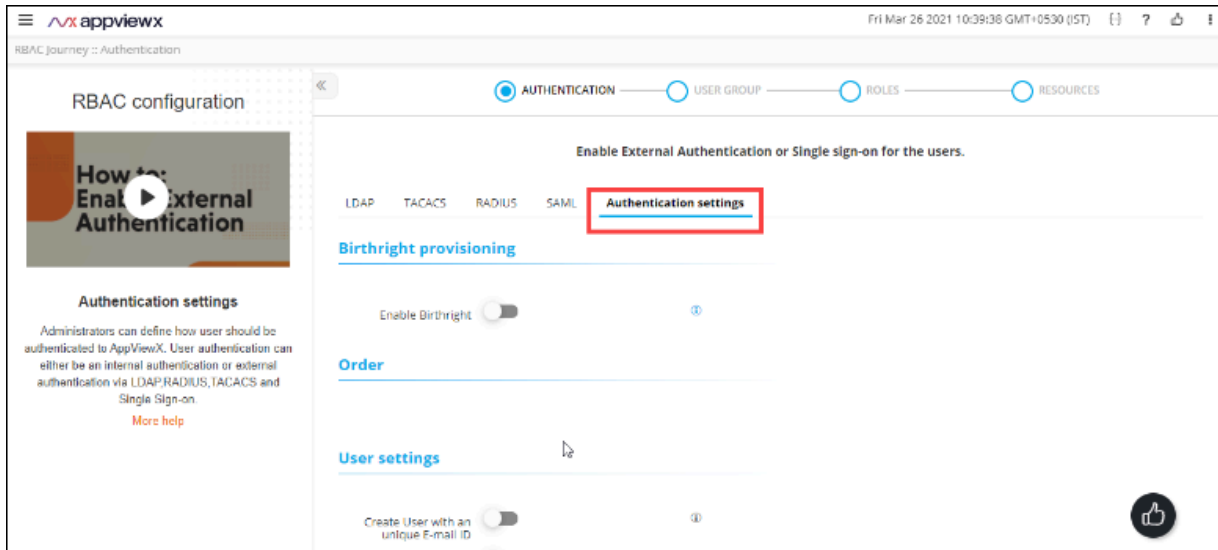
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



- From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.



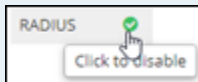
- On the **RBAC Journey :: Authentication** page, click the **Authentication Settings** tab.



7. To enable **Birthright provisioning** for new users who log into the system with a predefined set of permissions (associated with the user group), turn on the **Enable Birthright** toggle.
8. To define the order in which the authentication settings will be checked, in the **Order** section, drag and drop the authentication labels to the required corresponding levels.
If the level 1 check is set to Local and the level 2 check is set to LDAP, user credentials will be authenticated locally first and then on the LDAP server.



Note: You can also disable, and then enable a level of authentication. To do this, click the green tick



next to the server name.

9. In the **User settings** section, enter the required field information.

User settings

Create User with an unique E-mail ID

☐

Create User on Authorization Failure

☒

Session Timeout

The following table describes the field information in this section:

Field	Description
Create User an unique E-mail ID	To ensure that every AppViewX user has a unique email ID, turn on this toggle.
Create User on Authorization Failure	To create a user even if authorization fails (but the user is authenticated successfully), turn on this toggle.
Session Timeout	AppViewX lets you set a session timeout limit between 2 and 480 minutes. To set a web session timeout limit, enter the value in minutes.

10. If the AppViewX node password has been changed, in the **Node Settings** section, enter the updated Node Password.

Node settings

Node Password

Save

Cancel



Note: The value entered in the Node Password field should be the same as the node password. To apply the changes, restart the avx-config-server pod in every datacenter.

11. Click **Save**.

Resource

The resource allows you to specify access at a granular level across all the devices and modules of AppViewX listed in this section, where the permission definitions are independent of each other. The resources can be assigned only to a User group. The resources that are assigned to the user groups will automatically inherit the permissions associated with that resource. User groups can be assigned more than one resource.

AppViewX enables the following resource-related features:

- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query using object/Certificate fields available within in AppViewX.
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates using a script to tag based on data available with external tools (SNOW, Other CMDB, etc.).
- Rule templates are pre-shipped to ease the rule creation to dynamically tag resources.
- Dynamically created resources can be assigned to user groups dynamically by mapping the respective rule to the required user groups as part of the Rules in Use inventory in the wizard flow.
- Manage the order of execution for the RBAC rules.
- Manage short circuit option to dynamically tag ADC objects



Note: This dynamic resource tagging is only for newly discovered ADC objects and certificates.



Note: Objects/Certificates and the respective permissions part of the existing resources will not be updated/changed.

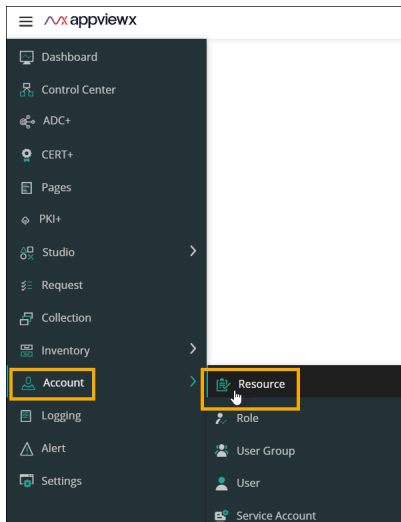
- [Create an RBAC Rule to Tag ADC Objects Using a Query](#)
- [Configuring a Variable as a Filter Condition Value based on Patterns](#)
- [Configuring the Resource Name](#)
- [Create an RBAC Rule to Tag ADC Objects/Certificates using a Script](#)
- [Configuring the Certificate Group Name](#)

- Configuring the Resource Name Based on Patterns
- Clone a Rule
- Delete a Rule
- RBAC Rule Mapping to User Groups to Dynamically Provide Access for Resources to User Groups
- Managing Order of Execution and Short Circuit Configuration for Rules

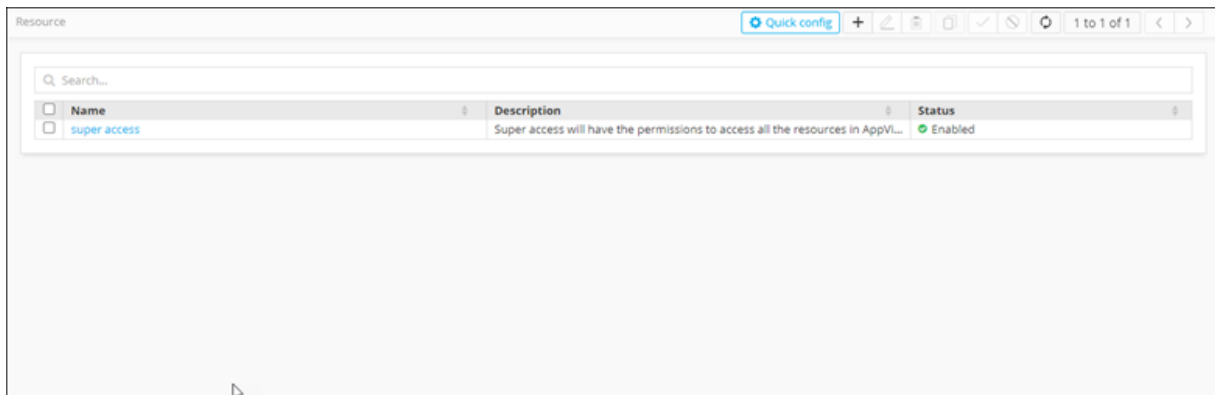
Create an RBAC Rule to Tag ADC Objects Using a Query

To create a RBAC rule to tag resources using a query:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Resource**.



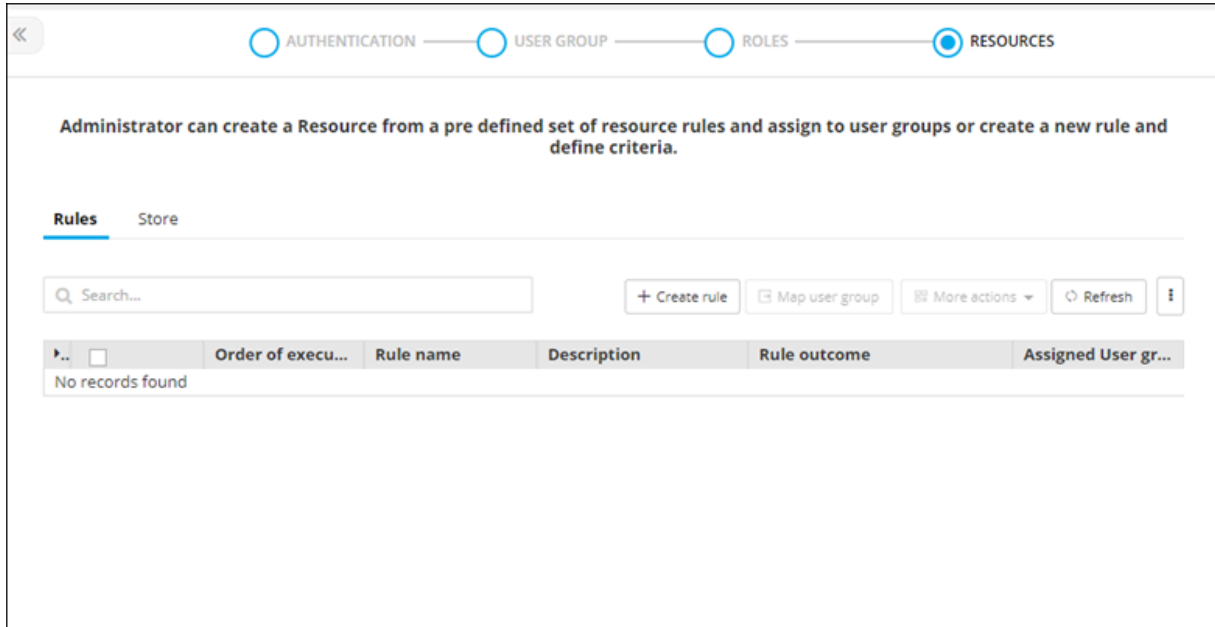
The **Resource** page is displayed.



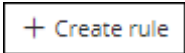
3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



5. Click



The **Rules :: Create** screen is displayed.

Navigation: << AUTHENTICATION USER GROUP ROLES **RESOURCES**

Rule Details

* Rule name

Rule Description

Rules

☒ ADC Rule
 ☐ Query
 ☐ Script
 Clear rule

☒ Certificate Rule
 ☐ Query
 ☐ Script
 Clear rule

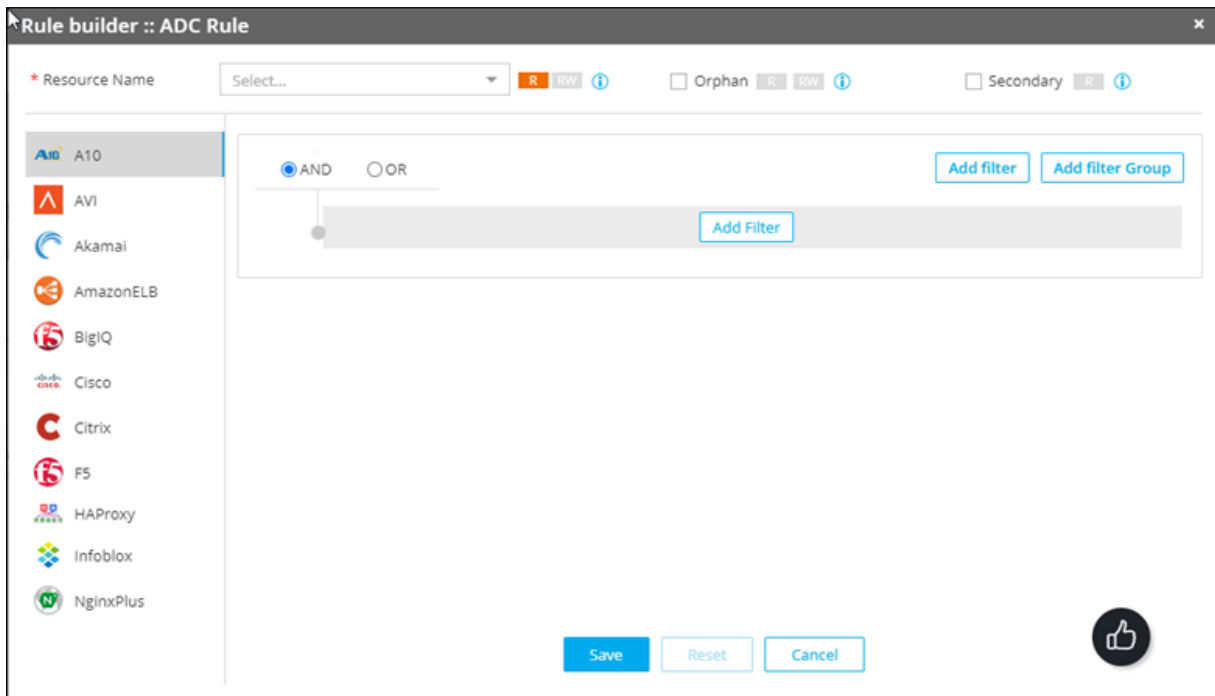
Save Cancel

6. In the **Rule Details** section, enter the following details:

Field	Description
*Rule Name	Resource name.
Rule Description	Brief description of the resource/granular level accesses associated with the resource.
All * marked fields are mandatory.	

7. To configure a rule to dynamically tag ADC objects using Query, in the **Rules** section, for the **ADC Rule**, select **Query**.

8. The **Rule builder :: ADC Rule** action pane is displayed.



9. On the **Rule builder :: ADC Rule** action pane, click **Add Filter**.
10. Select the field, condition and enter the value to be monitored for dynamic tagging of ADC objects based on rule condition.

Configuring a Variable as a Filter Condition Value based on Patterns

A variable can be defined with a pattern as specified below:

1. Select any one required field, then select condition as "Variable", define value in the format of < %variable%>. Example: A virtual server configured with the pattern vs_prod_support.appviewx.com can be defined as vs_<%variable1%>_support.appviewx.com [where <%variable1%> can match to name UAT, DEV, etc.].
2. Multiple variable definitions for the same object pattern can be defined as. vs_<%variable1%>_< %variable2%>_support.appviewx.com [where <%variable1%> can match to name UAT,DEV etc and < %variable2%> can match to name sales,marketing etc].
3. Variables can be used only across one field in a Rule.
4. Variable name should follow the below standards:
 - Only alphanumerics [A-Z, a-z, 0-9].
 - Special characters underscore [_].
 - Placeholder is <% for beginning and %> for ending.
5. Specify a resource name.

Configuring the Resource Name

To create resources dynamically based on patterns, resource name can be configured in the following ways:

1. Provide the Resource Name of an existing resource by choosing the Resource Name from Drop Down.
2. Provide a Static Name to the Resource. [When Rule matches the Resource Name would be created on Demand].
3. Provide a Pattern for the Resource Name. [Provide the variable pattern defined in the Query as the Resource Name].
4. Click either the **R** (Read-only) or **RW** (Read/Write) button to designate whether user groups assigned to the resource have read-only or read/write permissions on the ADC objects.

The ADC objects tagging has two additional fields that allow you to assign global permissions for orphan and secondary ADC objects to the resource you are creating. Users cannot assign individual permissions to orphan and secondary objects.

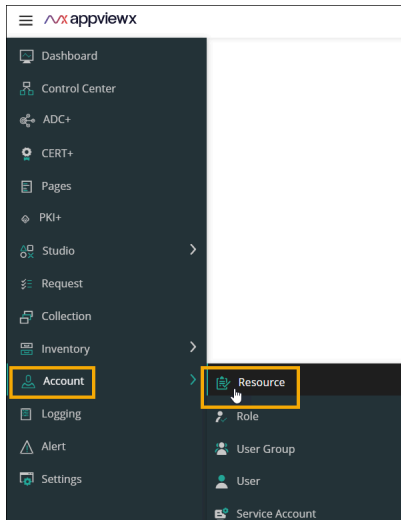
To enable this:

- a. Next to the **Resource** name, select the checkbox beside Orphan if you want to assign global permissions for orphan objects.
- b. Click either the **R** or **RW** icon to give users assigned to the resource Read-Only or Read/Write permissions on all orphan objects.
- c. Select the checkbox beside Secondary if you want to assign global permissions for secondary objects.
- d. Click the **R** icon to give user groups assigned to the resource Read-Only permissions on all secondary objects. The **RW** icon is not available because you cannot grant Read/Write access to secondary objects.
- e. Click **Save**.
- f. Saved rules will be displayed in the **Rules** tab.
- g. Go to the Rules tab by clicking on Resource in the breadcrumb.
- h. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
- i. Enable the rule by clicking on the respective status icon for the rule to be actively running.

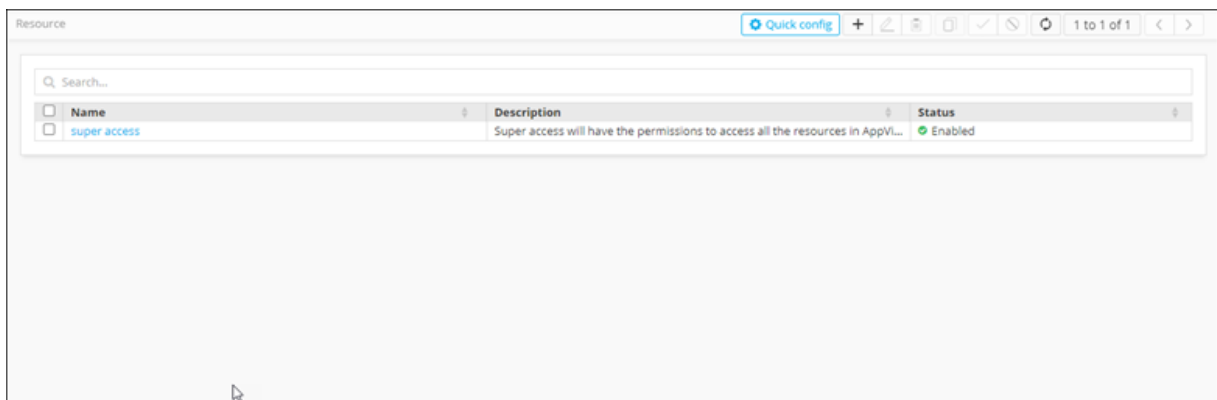
Create an RBAC Rule to Tag ADC Objects/Certificates using a Script

To create a RBAC rule to tag ADC objects/certificates using a script:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.

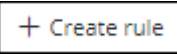
Administrator can create a Resource from a pre defined set of resource rules and assign to user groups or create a new rule and define criteria.

Rules Store

Search...

+ Create rule Map user group More actions Refresh

Order of execu...	Rule name	Description	Rule outcome	Assigned User gr...
No records found				

5. Click .

The **Rules :: Create** screen is displayed.

Rule Details

* Rule name

Rule Description

Rules

☒ ADC Rule
 ☐ Query
 ☐ Script
 Clear rule

☒ Certificate Rule
 ☐ Query
 ☐ Script
 Clear rule

Save Cancel

6. In the **Rule Details** section, enter the following details:

Field	Description
*Rule Name	Resource name.
Rule Description	Brief description of the resource/granular level accesses associated with the resource.
All * marked fields are mandatory.	

- To configure a rule to dynamically tag ADC objects using Query, in the **Rules** section, for the **ADC Rule**, select **Script**.
- Configure the details of the script, provide a resource name and assign required permissions. For ADC Objects, Orphan and Secondary objects need to be assigned globally. For Certificates, Certificate Group Name need to be provided.
- Click **Save**.
- Saved rules will be displayed in the **Rules** tab.
- Go to the Rules tab by clicking on Resource in the breadcrumb. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
- Enable the rule by clicking on the respective status icon for the rule to be actively running.

Configuring the Certificate Group Name

To create certificate groups dynamically based on patterns, the certificate group name can be configured in the following ways:

- Provide the certificate group name of an existing resource by choosing the certificate group name from the drop-down menu.
- Provide a Static Name to the certificate group name. [When Rule matches the Resource Name would be created on Demand].
- Provide a Pattern for the certificate group name. [Provide the variable pattern defined in the Query as the Resource Name].

For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>

Configuring the Resource Name Based on Patterns

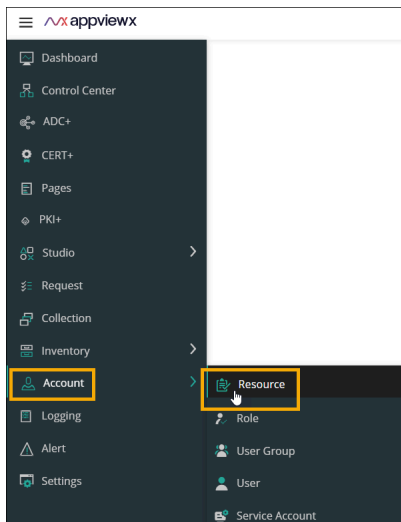
To create resources dynamically based on patterns, the resource name can be configured in the following ways:

- Provide the Resource Name of an existing resource by choosing the Resource Name from Drop Down.
- Provide a Static Name to the Resource. [When Rule matches the Resource Name would be created on Demand].
- Provide a Pattern for the Resource Name. [Provide the variable pattern defined in the Query as the Resource Name]. For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>.
- Click either the R (Read-only) or RW (Read/Write) button to designate whether user groups assigned to the resource have read-only or read/write permissions on the certificate groups.
- When you are finished configuring the Certificate rule, click Save. Saved rules will be displayed in the Rules tab.
- Go to the Rules tab by clicking on Resource in the breadcrumb. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
- Enable the rule by clicking on the respective status icon for the rule to be actively running.

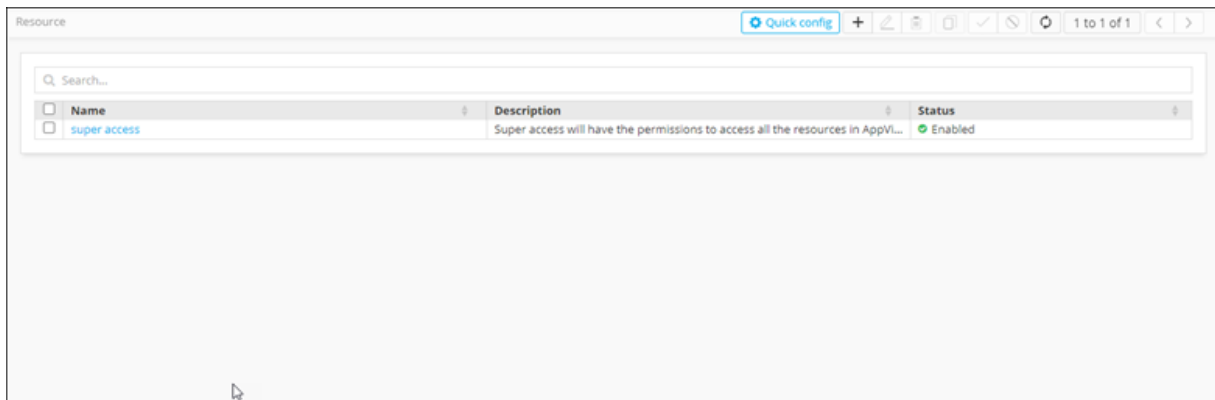
Clone a Rule

To clone a rule:

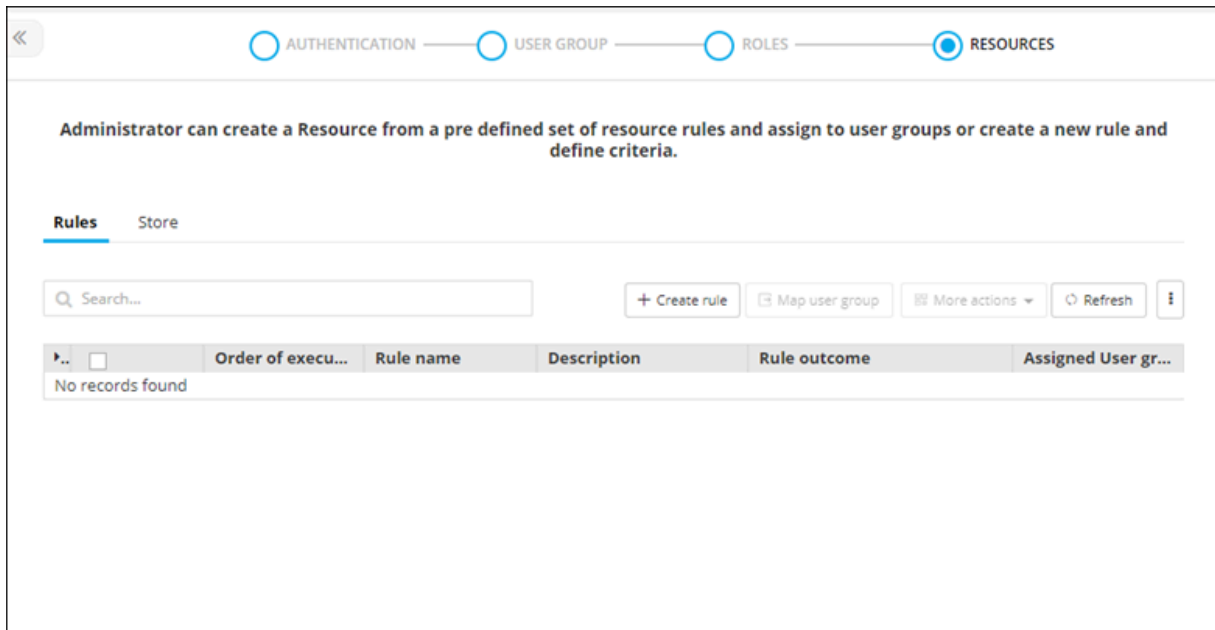
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.

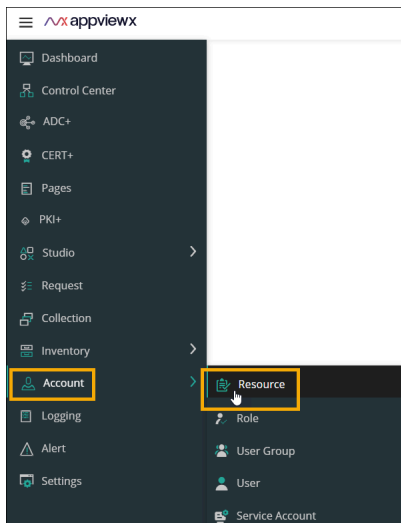


5. For the resource you want to clone, select the check box against that resource.
6. From the **More actions** drop-down menu, click **Clone**.
7. In the **Clone** rules dialog box, enter a name for the cloned rule and click **Save**.
Rule details will be closed and will be opened in edit mode for any further modification on description/ rule conditions.
8. Once the rule is saved, enable the rule by clicking on the respective status icon for the rule to be actively running in the rules inventory table.

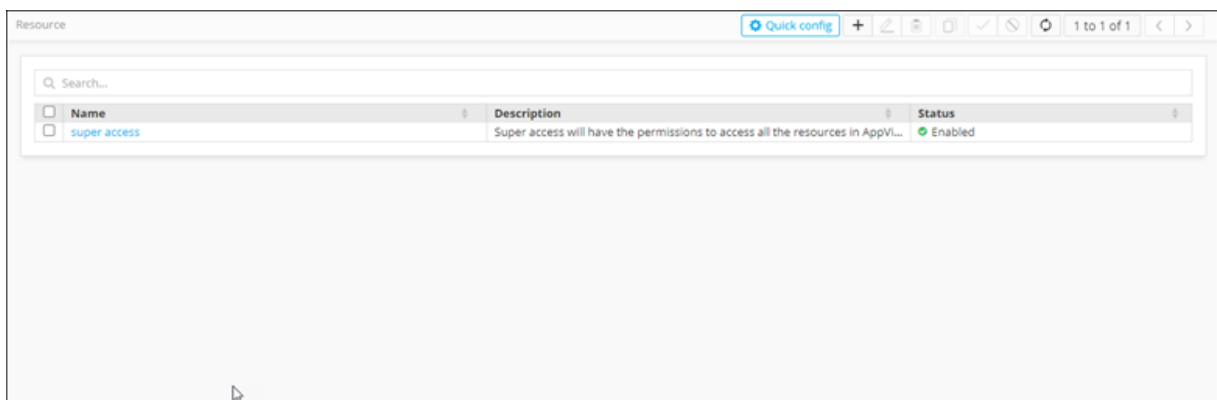
Delete a Rule

To delete a rule:

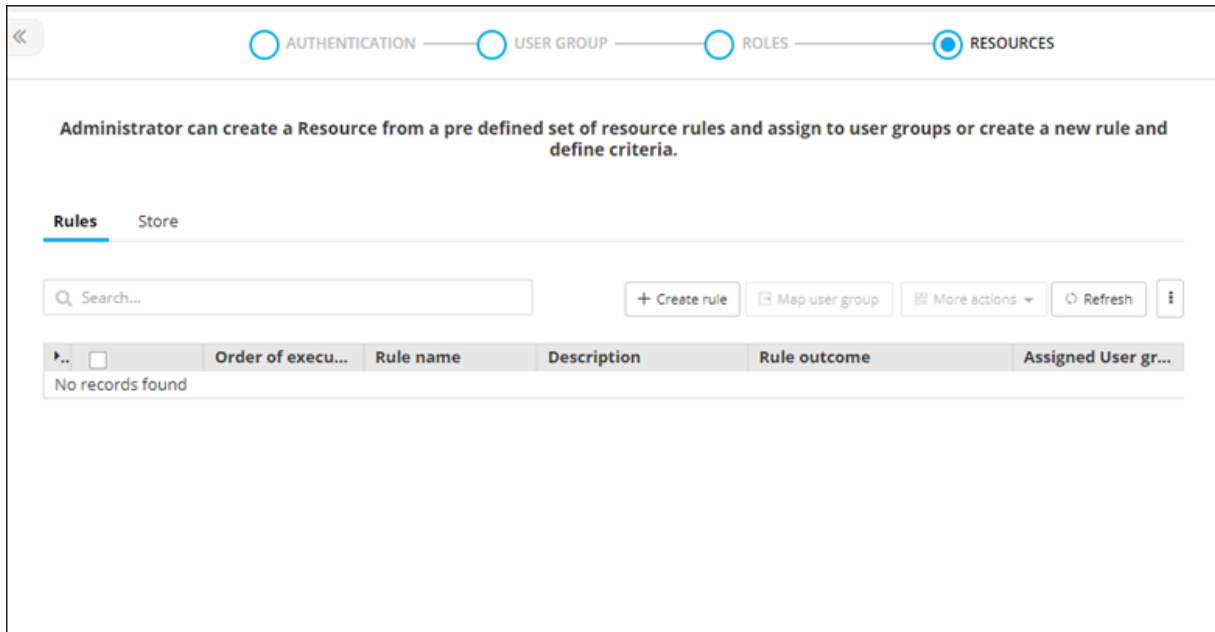
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.

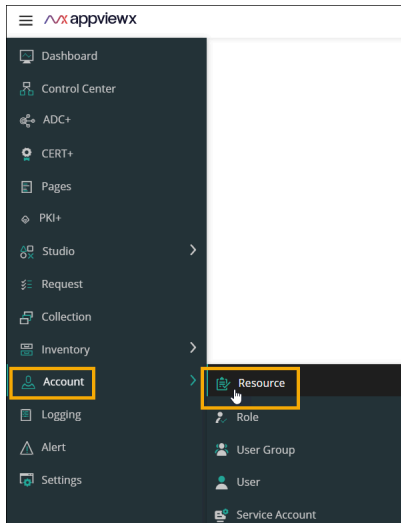


5. For the resource you want to delete, select the check box against that resource.
6. From the **More actions** drop-down menu, click **Delete**.
7. In the **Confirmation** dialog box, click **Yes**.

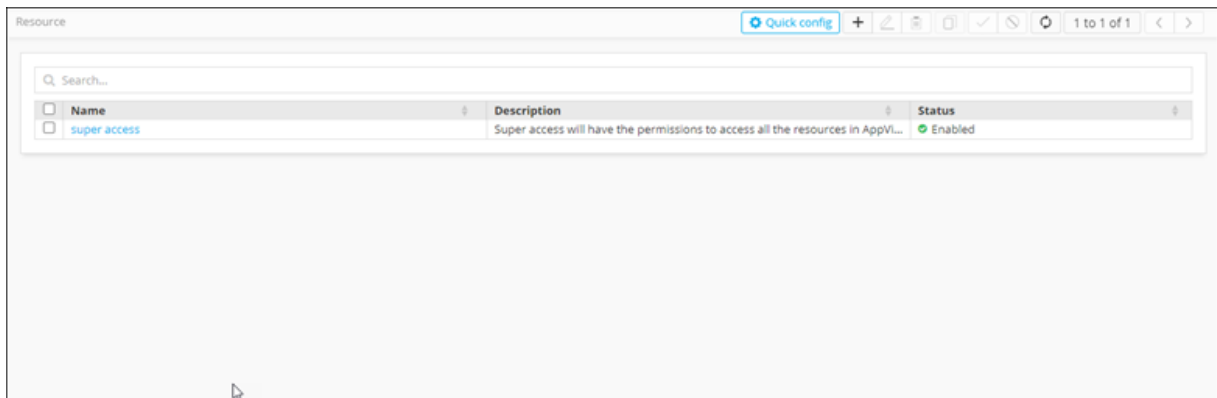
RBAC Rule Mapping to User Groups to Dynamically Provide Access for Resources to User Groups

To create a RBAC rule to dynamically provide access for resources to user groups:

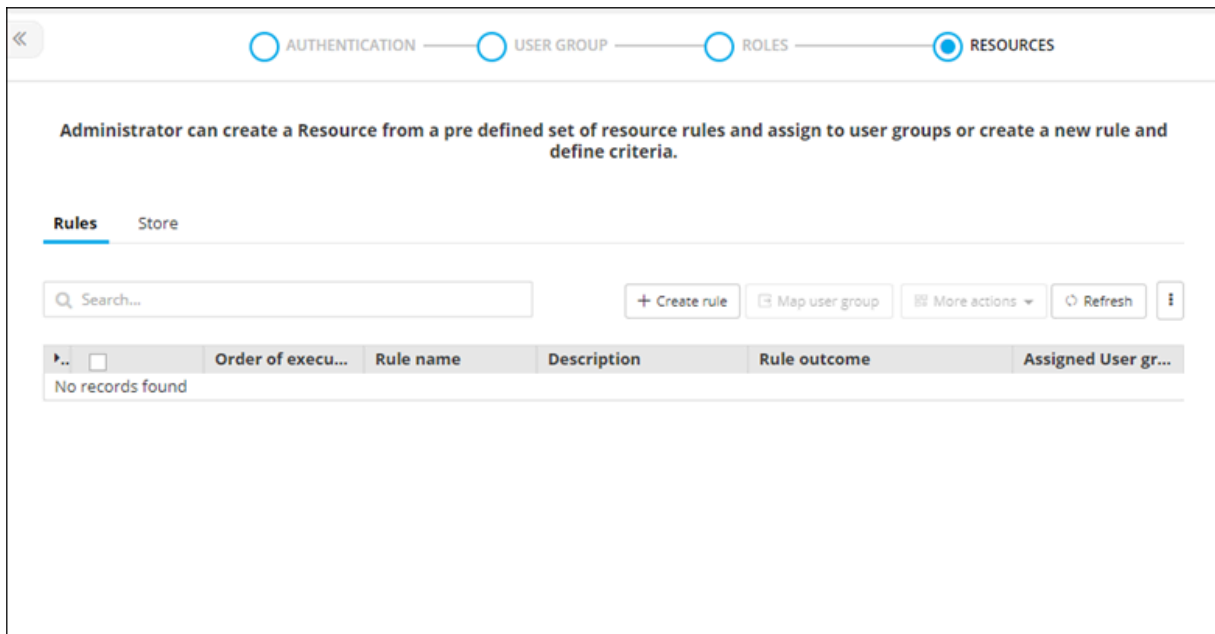
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



5. For the resource you want to map to user groups, select the check box against that resource.



6. Click

7. In the **Map user group** action pane, select the user groups the resource will be mapped to.

8. Click **Save**.

Managing Order of Execution and Short Circuit Configuration for Rules

For managing the order of rule execution to avoid conflicts across multiple rules matching similar conditions and tag to expected resources:

- In the rule inventory table, click and hold a rule name and drag it up or down to change the order of execution of rules in use in the system.
- The order will be automatically saved OR Click the up or down arrows beside each rule name to update the rule execution order.

Key points for consideration:

- Order of execution needs to be maintained by the user only to manage certificates tagged to expected certificate groups configured part of a rule, as certificates can't be part of multiple certificate groups.
- Based on the order of execution and matching rule condition, certificates will be only tagged to the certificate group at the top of rule execution order even though other RBAC rules down the order have a matching condition.

- Order of execution also needs to be maintained by the user for ADC objects tagging to a specific resource only when Short circuit option is turned on for ADC.
- By default, a short circuit will be turned off for ADC as ADC objects can be tagged to multiple resources. There is no such restriction for ADC as it is existing for a certificate tagging. For certificates, a short circuit will always be turned on and can't be changed by the user.
- To enable a short circuit for ADC, click More icon under the Rules Inventory>> Enable Short Circuit for ADC.

Role

Each role assigns a specific set of permissions relating to the modules that can be accessed and the tasks that can be performed in each AppViewX module. The roles can be assigned only to a User group. The user groups that are assigned with a role will automatically inherit all the associated permissions. User groups can be assigned more than one role.

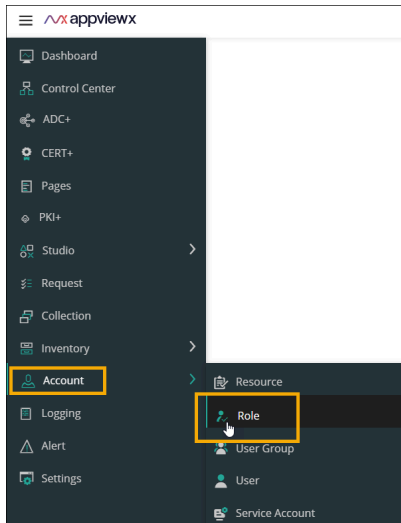
AppViewX enables the following role-related features:

- Out of the Box (OOB) roles are available for ADC, Certificates, Security, and Automation modules.
- OOB roles can be cloned, enabled, and disabled. OOB roles can't be updated/deleted.
- Administrators can also create custom roles. Custom roles can be updated, deleted, enabled and disabled.
- Users can either use OOB roles (if suits their needs) or custom roles to map to user groups.
- [Creating a Custom Role](#)
- [Cloning a Role](#)
- [Modifying a Role](#)
- [Enabling a Role](#)
- [Disabling a Role](#)
- [Mapping Role to User Groups](#)

Creating a Custom Role

To create a custom role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.



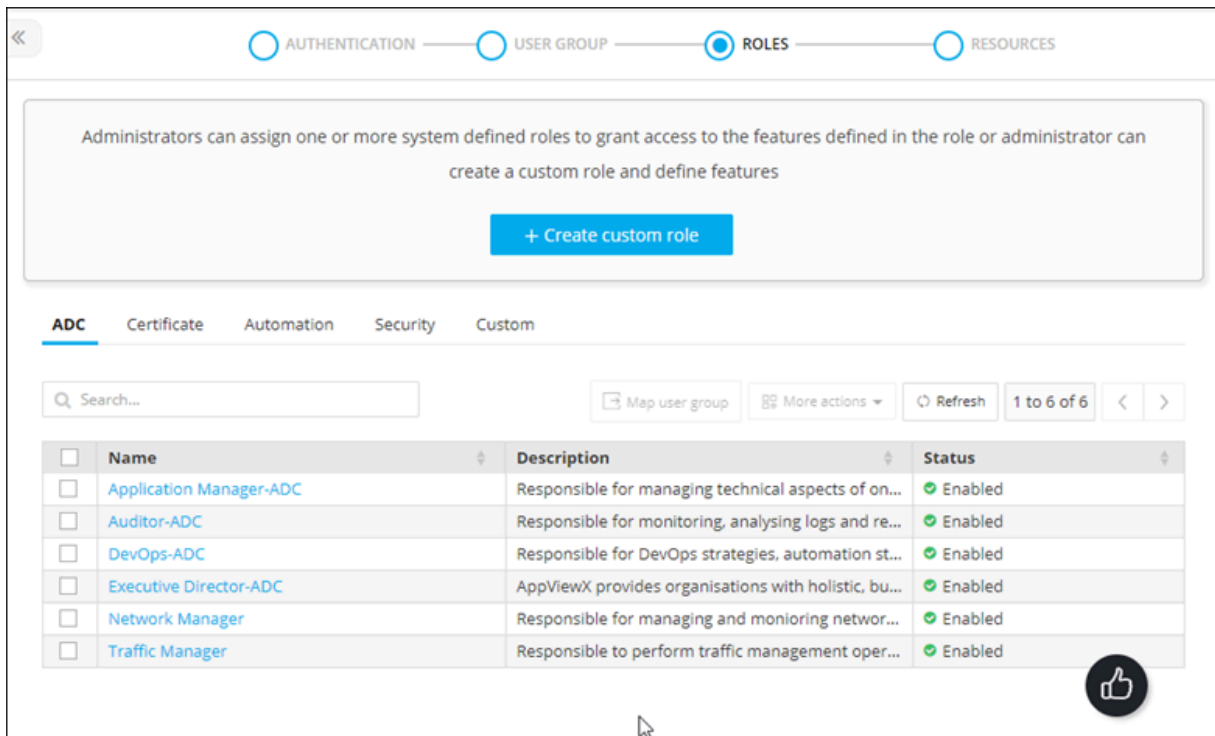
The **Role** page is displayed.

Quick config		
1 to 22 of 22		
☐	Name	Description
☒	Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...
☐	Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...
☐	Application Manager-User	Responsible to monitor the application specific certificates, setup alerts f...
☐	Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions
☐	Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions
☐	CA Manager	Responsible to manage CA related request and operations in AppViewX
☐	CA Manager Read Only	Responsible to view CA related request and operations in AppViewX
☐	CLM Manager	Responsible to manage AppViewX CLM Platform functions
☐	DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...
☐	DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign
☐	DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign
☐	Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Network Manager	Responsible for managing and monitoring network infrastructure
☐	Portal User	Responsible for Self-servicing and accessing automation flows via Catala...
☐	Security Manager	This role grants users complete access to all objects on the system
☐	Status	Enabled

3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



5. Click

+ Create custom role

The **Create custom role** action pane is displayed.

6. Under the **Information** tab, enter the following details:

Field	Description
*Name	Role name.
Description	Brief description of what users assigned to the role can do and/or what features or functionalities are associated with the role.
All * marked fields are mandatory.	

7. Click **Save**.

8. In the **Authorized functions** section, select the check box against the functionalities that you want to associate with the role.

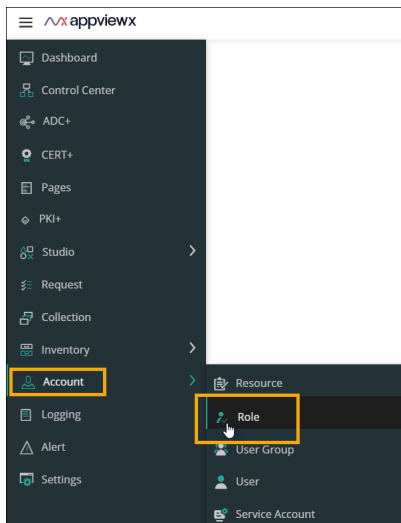
9. To assign functions at a granular level, click the  icon for the functions' check box and then select individual sub-options within the functions.

10. Click **Save**.

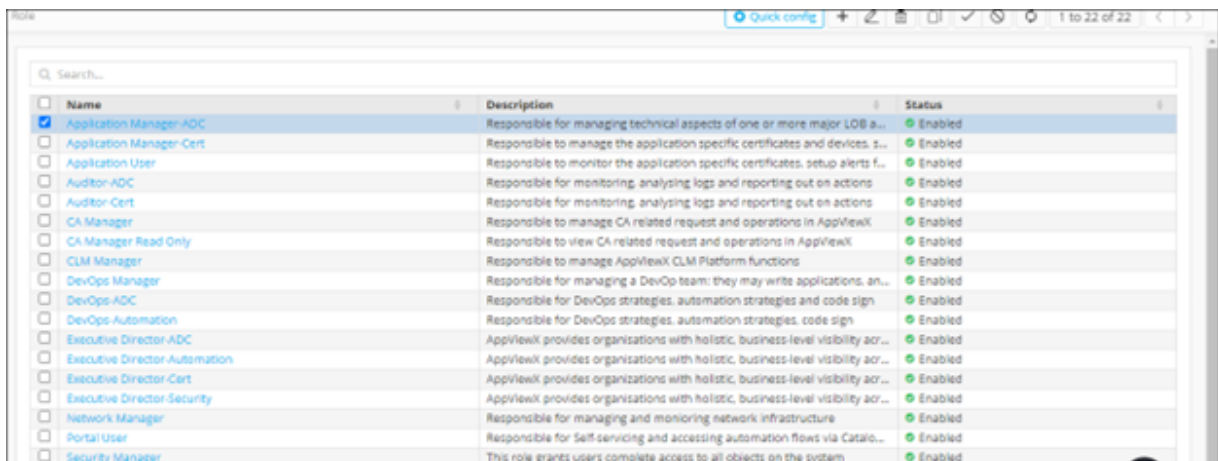
Cloning a Role

To clone an existing role to a custom role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.



The **Role** page is displayed.

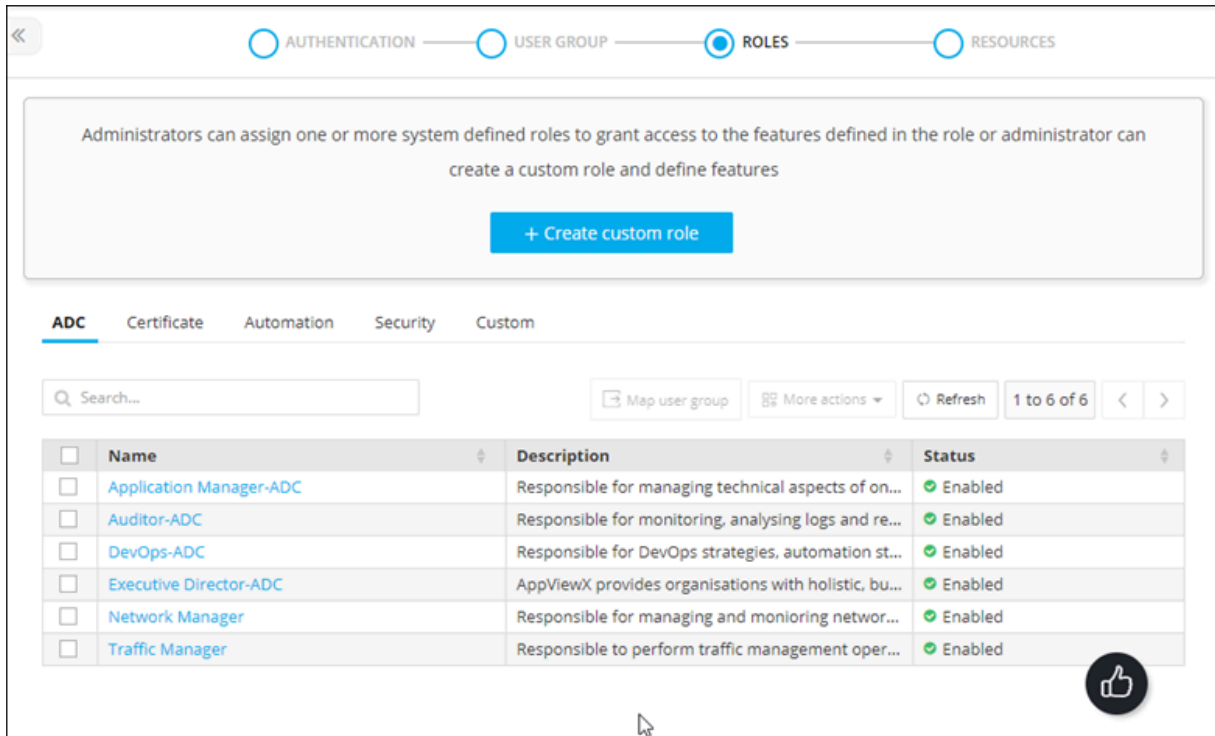


Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catale...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled

3. From the top-right corner of the screen, click **Quick Config**.

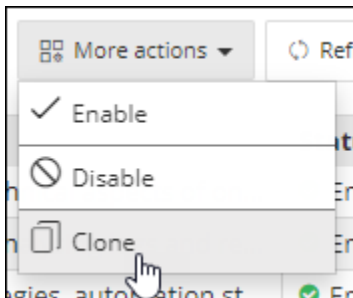
The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



5. For the role, you want to clone, select the check box against that role.

6. From the **More actions** drop-down menu, select **Clone**.



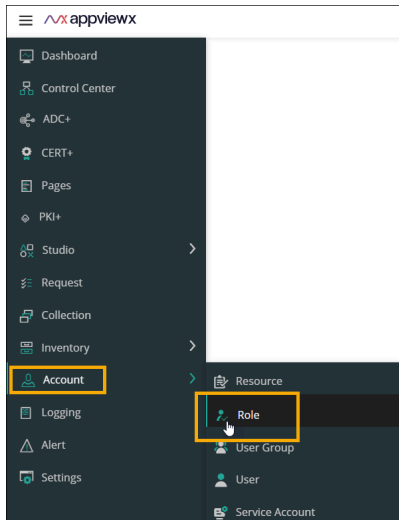
7. In the **Clone** action pane, modify the details in the **Information** and **Authorized functions** sections as required.

8. Click **Save**.

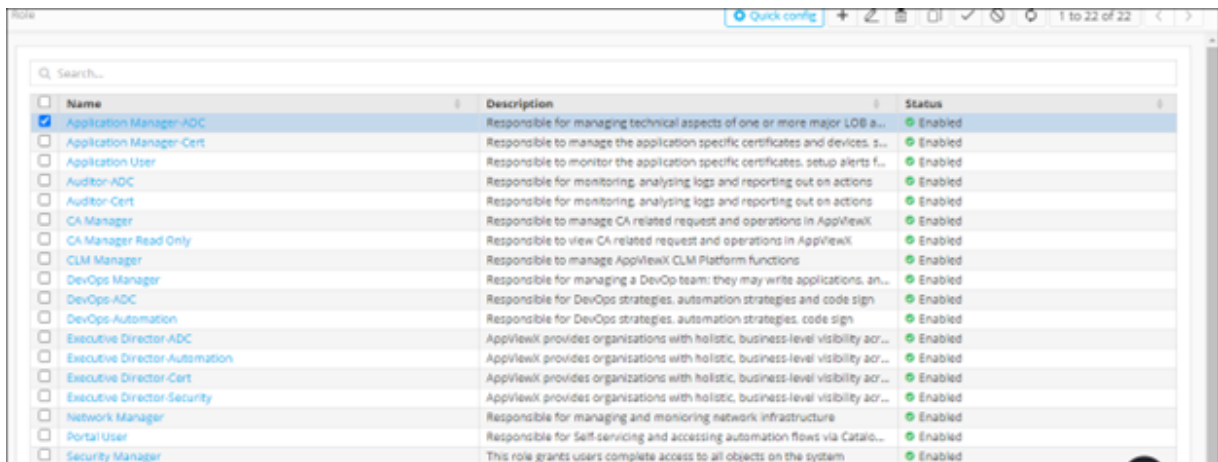
Modifying a Role

To modify a custom role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.

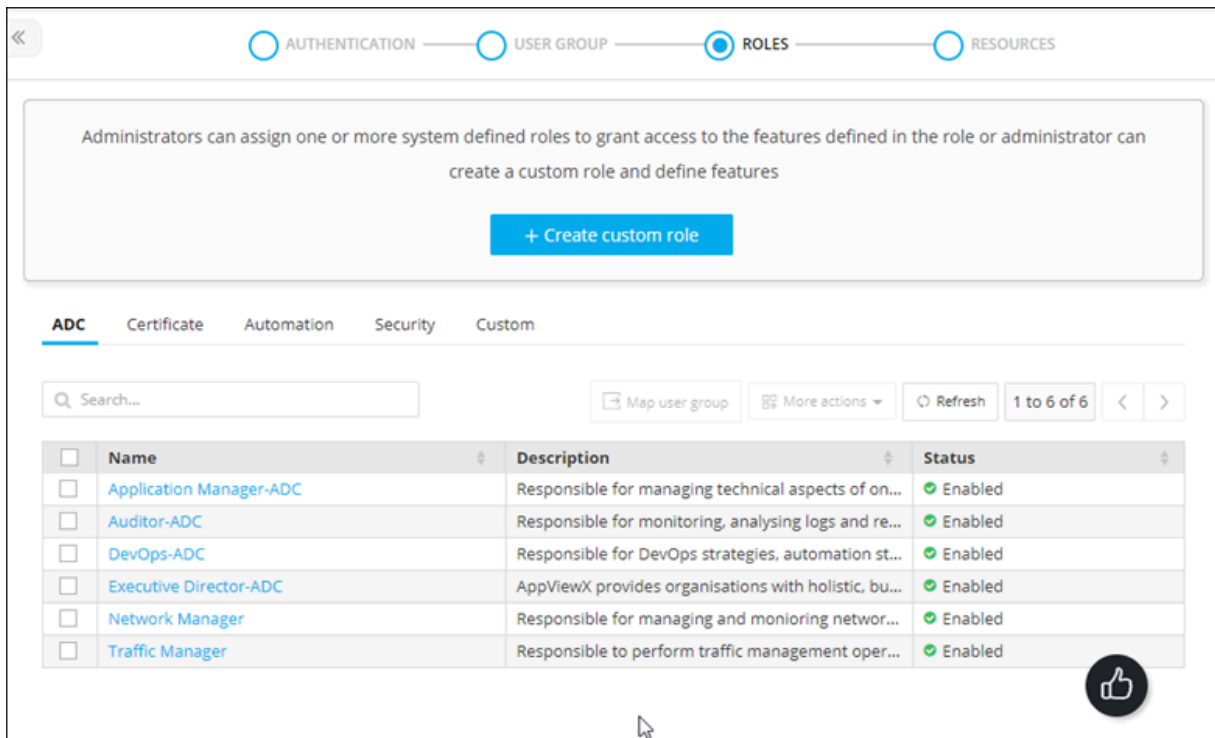


The **Role** page is displayed.



Name	Description	Status
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...	Enabled
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX.	Enabled
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX.	Enabled
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☐ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...	Enabled
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled

3. From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



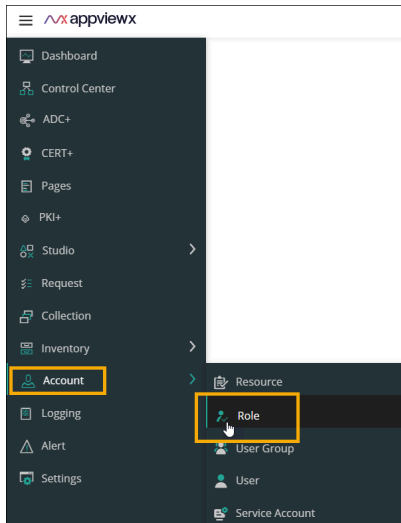
5. Click the role name you want to modify.
6. The **Edit role** action pane is displayed for the selected role.
7. Modify the details in the **Information** and **Authorized functions** sections as required.
8. Click **Save**.

 **Note:** Out of the box role functions can't be edited. Only custom role functions can be edited.

Enabling a Role

To enable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.



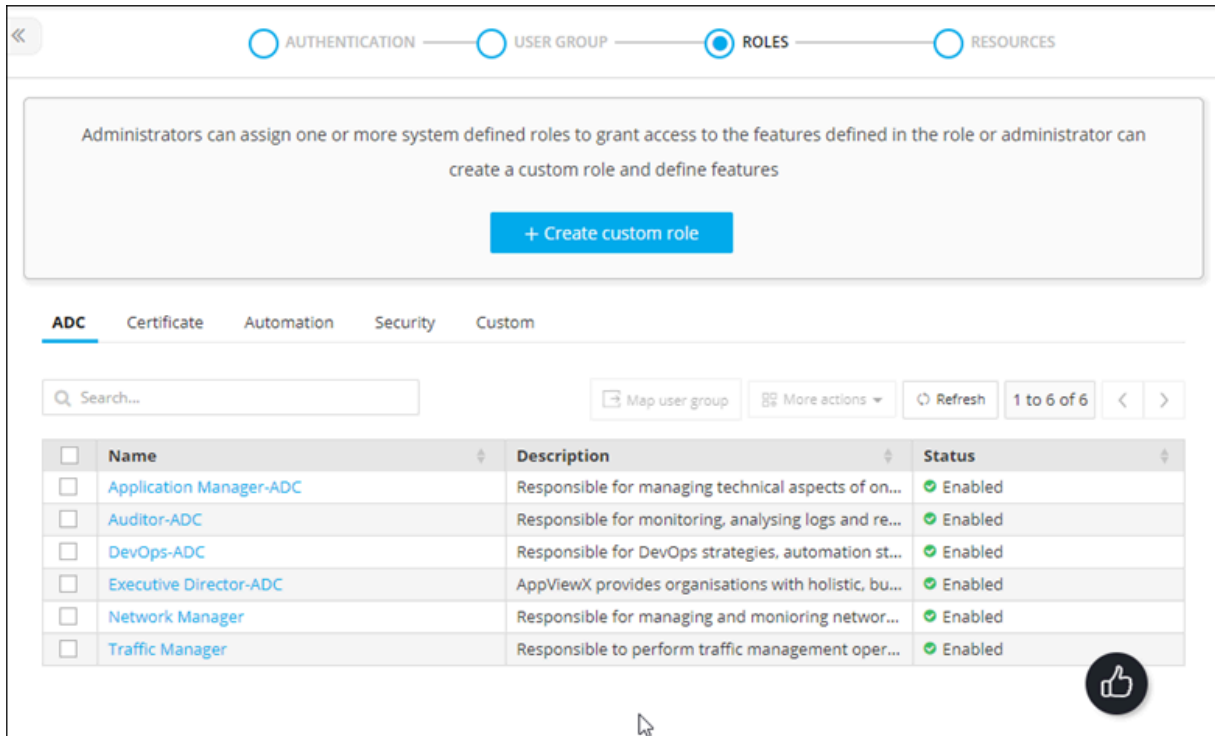
The **Role** page is displayed.

Quick config		
1 to 22 of 22		
☐	Name	Description
☒	Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...
☐	Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...
☐	Application Manager	Responsible to monitor the application specific certificates, setup alerts f...
☐	Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions
☐	Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions
☐	CA Manager	Responsible to manage CA related request and operations in AppViewX
☐	CA Manager Read Only	Responsible to view CA related request and operations in AppViewX
☐	CLM Manager	Responsible to manage AppViewX CLM Platform functions
☐	DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...
☐	DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign
☐	DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign
☐	Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Network Manager	Responsible for managing and monitoring network infrastructure
☐	Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...
☐	Security Manager	This role grants users complete access to all objects on the system
	Status	Enabled

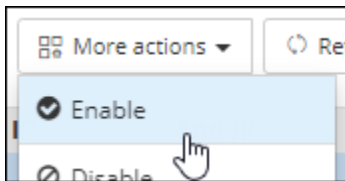
3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



5. To enable a role, select the check box against that role.
6. From the **More actions** dropdown menu, select **Enable**.



7. In the **Enable** role(s) dialog box, click **Yes**.

Disabling a Role



Note: You cannot disable roles that have active users associated with them.



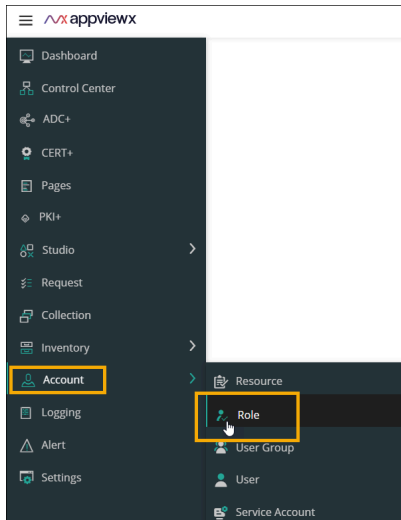
Note: The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the



2. From the menu displayed, click **Account > Role**.



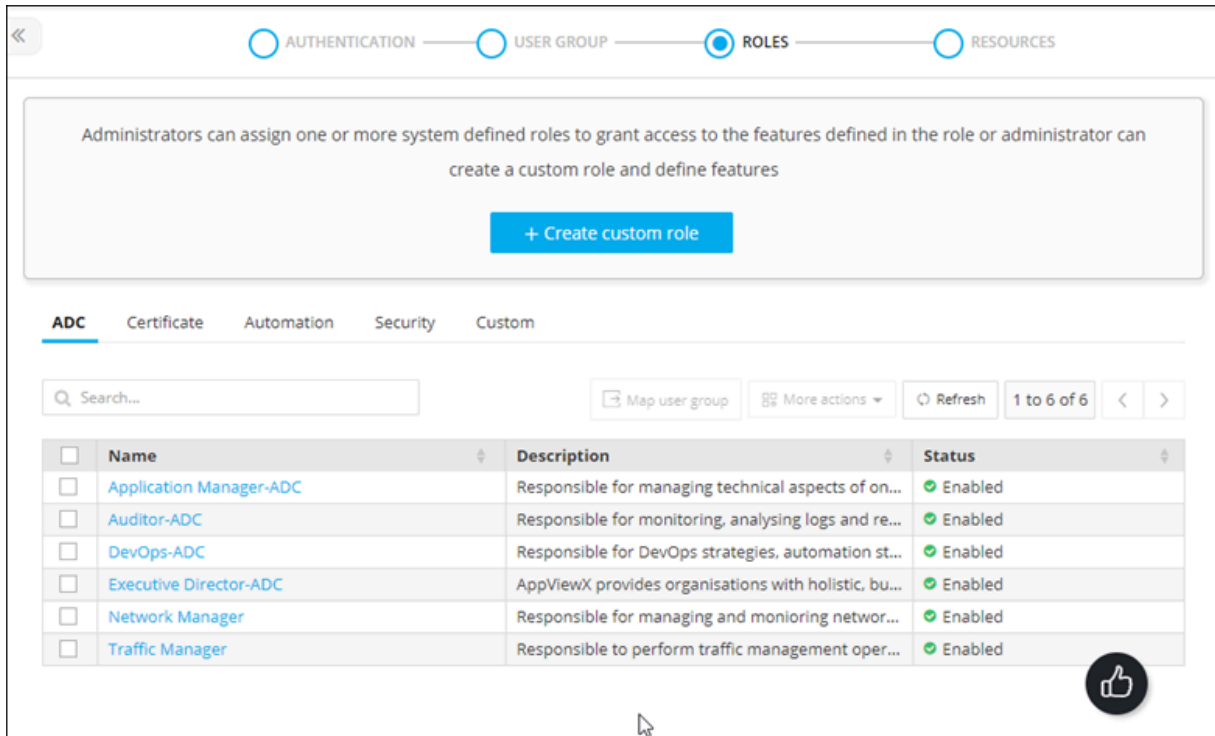
The **Role** page is displayed.

Role			
Quick config			
1 to 22 of 22			
Name	Description	Status	
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...	Enabled	
☐ Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...	Enabled	
☐ Application User	Responsible to monitor the application specific certificates, setup alerts f...	Enabled	
☐ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled	
☐ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled	
☐ CA Manager	Responsible to manage CA related request and operations in AppViewX.	Enabled	
☐ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX.	Enabled	
☐ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled	
☐ DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...	Enabled	
☐ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled	
☐ DevOps Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled	
☐ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled	
☐ Executive Director Automation	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled	
☐ Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled	
☐ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...	Enabled	
☐ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled	
☐ Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...	Enabled	
☐ Security Manager	This role grants users complete access to all objects on the system	Enabled	

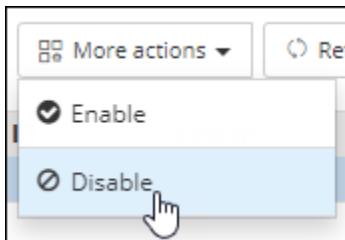
3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



5. To disable a role, select the check box against that role.
6. From the **More actions** dropdown menu, select **Disable**.

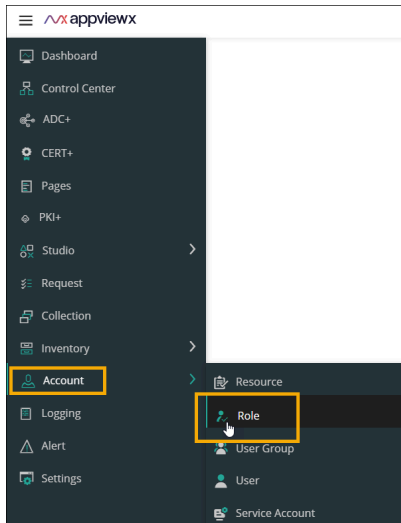


7. In the **Disable** role(s) dialog box, click **Yes**.

Mapping Role to User Groups

To map roles to user groups:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > Role**.



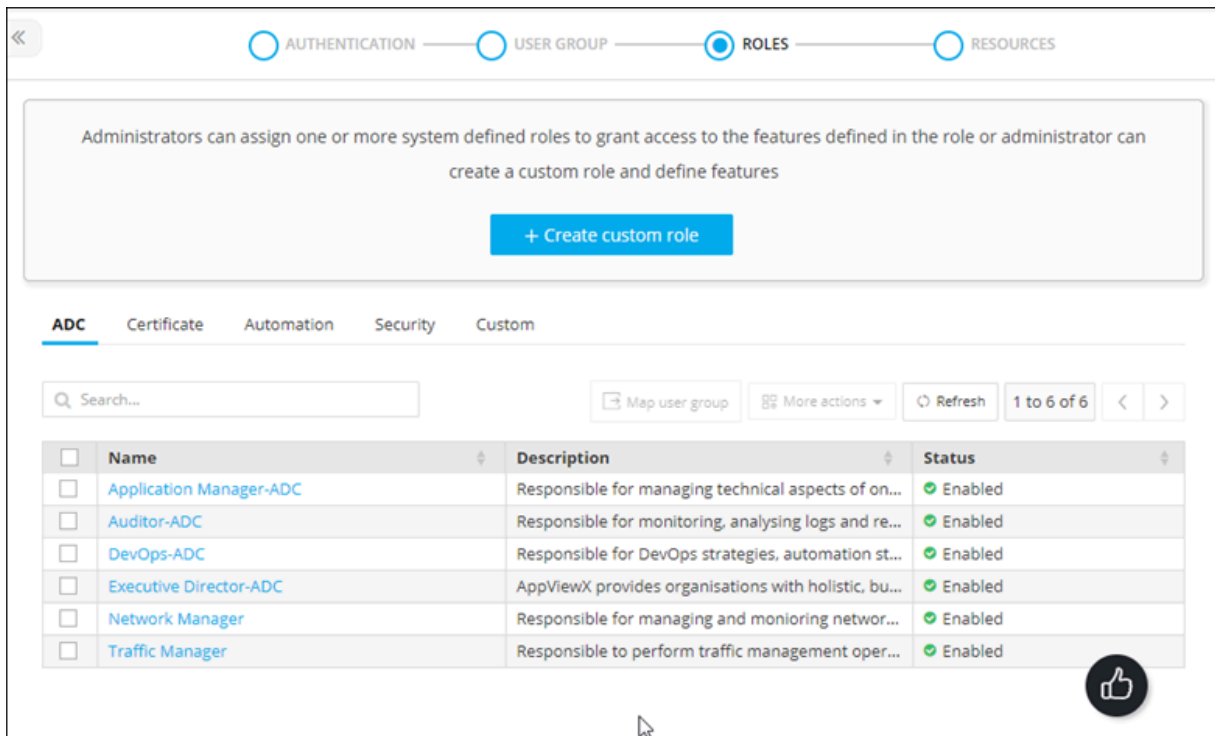
The **Role** page is displayed.

Quick config		
1 to 22 of 22		
☐	Name	Description
☒	Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB a...
☐	Application Manager-Cert	Responsible to manage the application specific certificates and devices. s...
☐	Application User	Responsible to monitor the application specific certificates, setup alerts f...
☐	Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions
☐	Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions
☐	CA Manager	Responsible to manage CA related request and operations in AppViewX
☐	CA Manager Read Only	Responsible to view CA related request and operations in AppViewX
☐	CLM Manager	Responsible to manage AppViewX CLM Platform functions
☐	DevOps Manager	Responsible for managing a DevOp team: they may write applications, an...
☐	DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign
☐	DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign
☐	Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Cert	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility acr...
☐	Network Manager	Responsible for managing and monitoring network infrastructure
☐	Portal User	Responsible for Self-servicing and accessing automation flows via Catalo...
☐	Security Manager	This role grants users complete access to all objects on the system
☐	Status	Enabled

3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



5. For the role, you want to map to user groups, select the check box against that role.



6. Click

7. In the **Mapping user group** action pane, select the user groups the role will be mapped to.

8. Click **Save**.

The saved list of user groups will be displayed as a hyperlink in the rule inventory for each group.

User Group

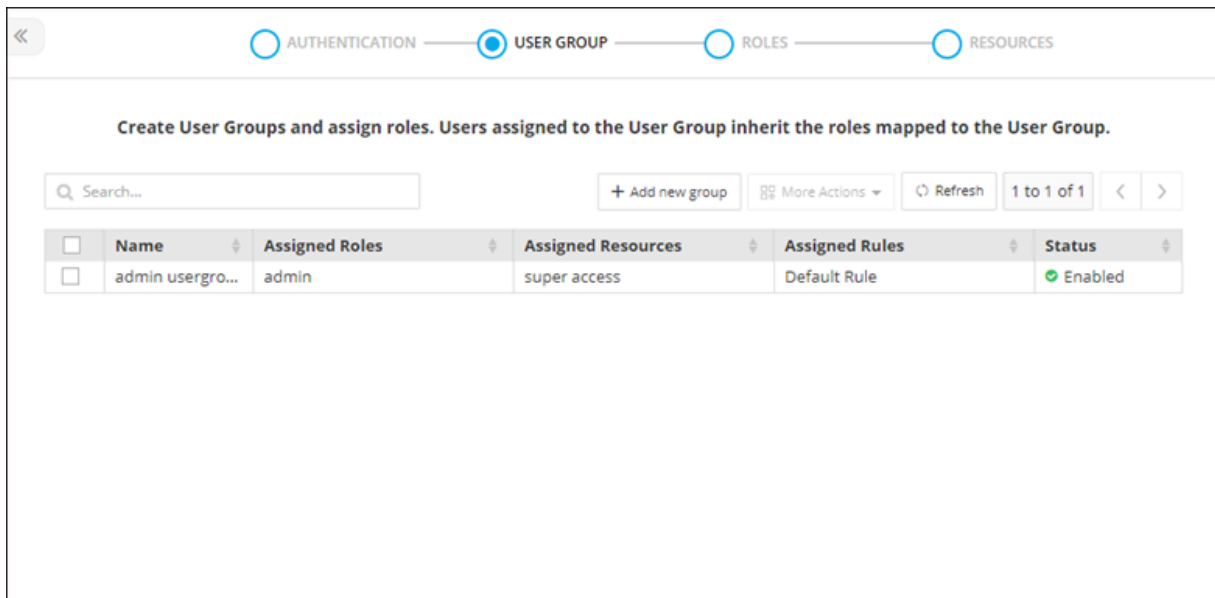
A user group is a group of individuals that have access to the same roles and resources. When you associate a role and resource with a user group, the users within that user group are granted all of the roles and resources' corresponding privileges and permissions. User Groups can be created manually or synced from the Active Directory or can be bulk uploaded using a spreadsheet.



Note: You can associate the roles and resources only with the user groups.

Once Authentication details are configured:

1. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



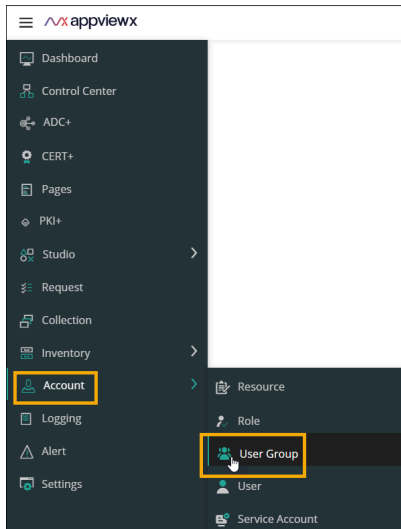
2. The User group inventory table is displayed with the list of available user groups in AppViewX along with corresponding roles and resources mapping.
3. In the User group stage, user group creation can be done by fetching groups from LDAP or through bulk import.
4. In addition to this, existing user groups can be cloned, enabled, disable, and deleted.

- [Adding a New User Group by Syncing Groups from LDAP](#)
- [Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option](#)
- [Add New User Group by Bulk Import](#)
- [Cloning a User Group](#)
- [Enabling a User Group](#)
- [Disabling a User Group](#)
- [Deleting a User Group](#)

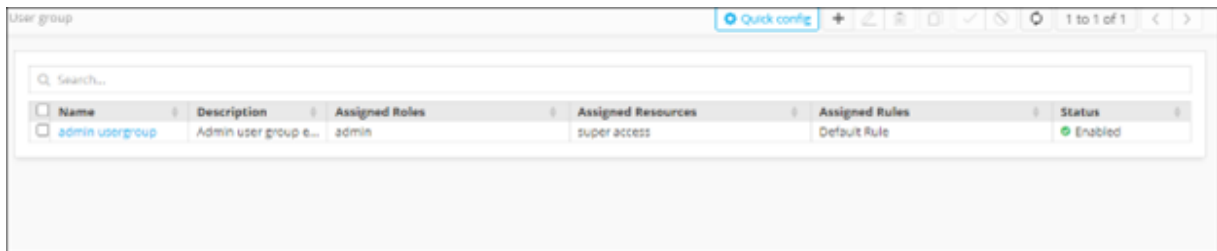
Adding a New User Group by Syncing Groups from LDAP

To create a new user group by syncing groups from LDAP:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User Group**.



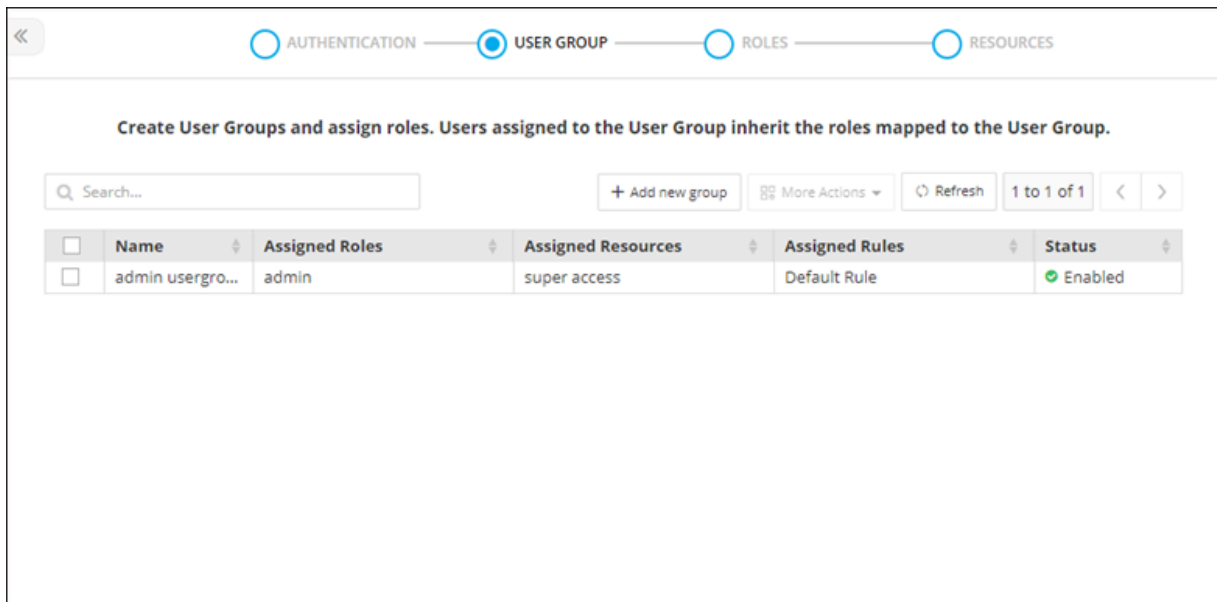
The **UserGroup** page is displayed.



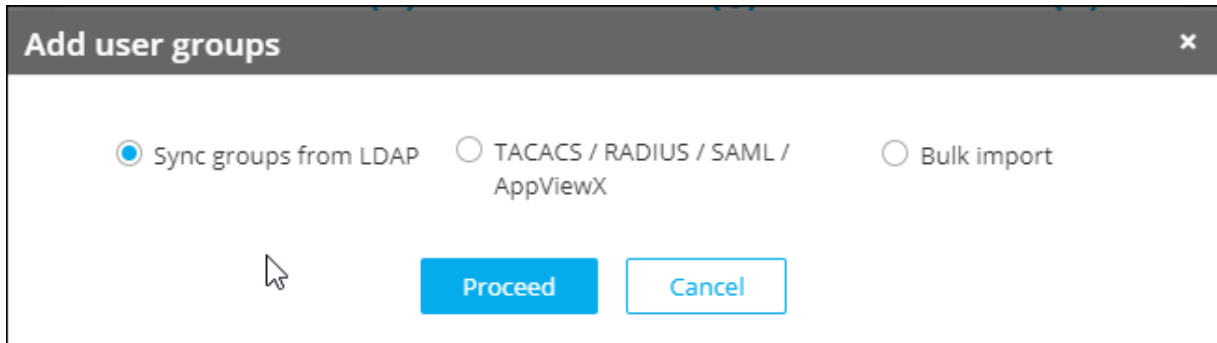
3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



5. Click .
6. From the **Add user groups** dialog box, select **Sync groups from LDAP** and click **Proceed**.



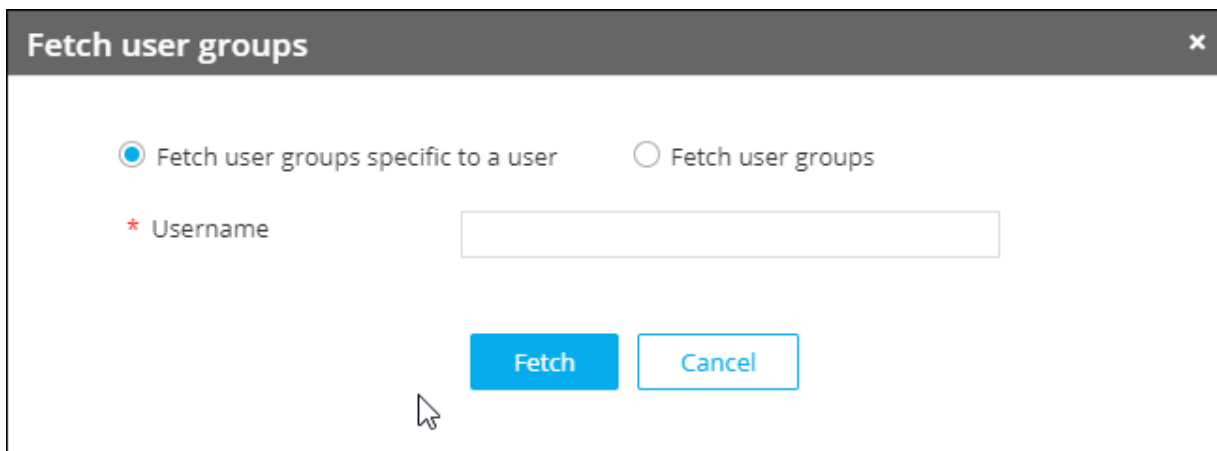
The **Add user groups** dialog box is shown. It has a title bar with a close button. Inside, there are three radio buttons: **Sync groups from LDAP** (selected), **TACACS / RADIUS / SAML / AppViewX**, and **Bulk import**. At the bottom, there are two buttons: **Proceed** and **Cancel**.

The LDAP inventory table is displayed.

7. To view the user groups available in the AD and create or map them with the existing user groups in

AppViewX, from the LDAP inventory table, click .

The **Fetch user groups** dialog box is displayed.



The **Fetch user groups** dialog box is shown. It has a title bar with a close button. Inside, there are two radio buttons: **Fetch user groups specific to a user** (selected) and **Fetch user groups**. Below the first radio button, there is a label *** Username** and an empty text input field. At the bottom, there are two buttons: **Fetch** and **Cancel**.

8. In the **Fetch user groups** dialog box:
- To fetch user groups according to a specific user, select **Fetch user groups specific to a user** and enter the **Username** of the AD user.
 - To fetch user groups by a specific name, select **Fetch user groups** and type the enter the **User group name** from the AD.

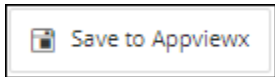


Note: You can search the user group either by entering the complete user group name or using wild card characters (*).

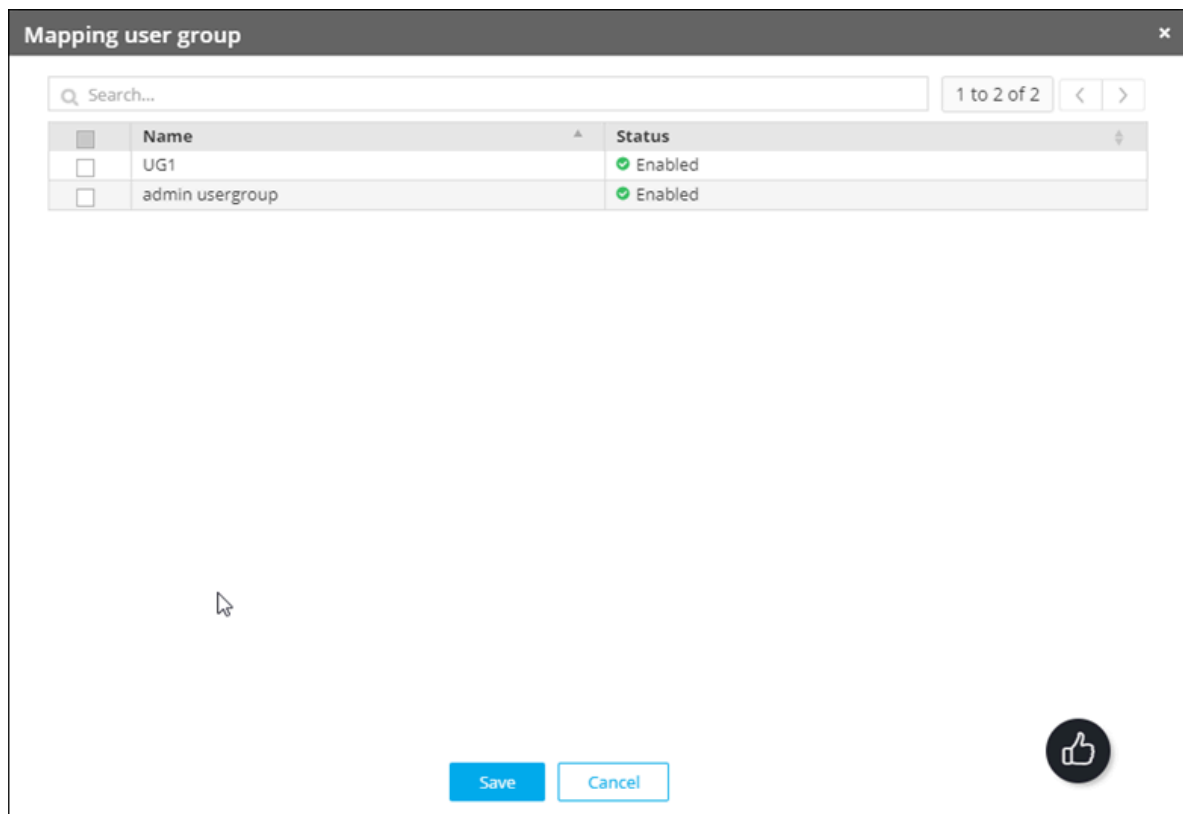
9. Click **Fetch**.

A table containing the AD group names and their corresponding AppViewX user group names is displayed.

10. Select the AD user group(s) that must be created with the same name in AppViewX and click



11. To select the AD user group(s) to be mapped with the existing AppViewX user group:
- Select the user group to be mapped with the existing AppViewX user group.
 - From the **More actions** list, select **Create Map**.
 - From the **Mapping user group** action pane, select the existing AppViewX user group to be mapped.



- d. Click **Save**.

Selected AD user group(s) will be now mapped to the existing AppViewX user group and the same mapping will reflect in the AD group names table.

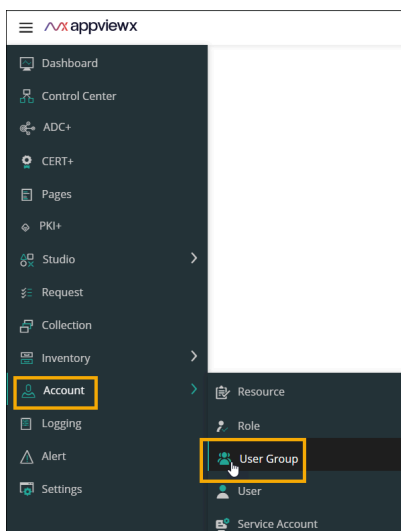
12. To export specific AD groups:

- a. Select the user group to be mapped with the existing AppViewX user group. From the **More actions** list, select **Export**.
- b. From the **Export user groups** action pane, select the Selected group(S) option and click **Yes** or to export all user groups, select the **All User Group(s)** option and click **Yes**.
- c. The selected/all user group(s) should be automatically exported in (.CSV) Format.

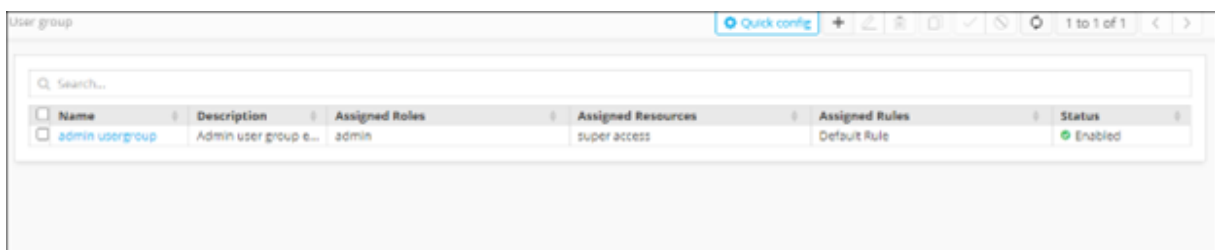
Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option

To create a new user group using the TACACS/RADIUS/SAML/AppViewX option:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User Group**.



The **UserGroup** page is displayed.



Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled

3. From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.

Navigation: << AUTHENTICATION — USER GROUP — ROLES — RESOURCES

Create User Groups and assign roles. Users assigned to the User Group inherit the roles mapped to the User Group.

Search:

Buttons: + Add new group, More Actions, Refresh, 1 to 1 of 1, <, >

☐	Name	Assigned Roles	Assigned Resources	Assigned Rules	Status
☐	admin usergro...	admin	super access	Default Rule	Enabled

- Click **+ Add new group**.
- From the **Add user groups** dialog box, select **TACACS/RADIUS/SAML/AppViewX** and click **Proceed**.
- Enter the **Name** and **Description** for the user group.

Add user groups [X]

☐ Sync groups from LDAP
 ☒ TACACS / RADIUS / SAML / AppViewX
 ☐ Bulk import

* Name

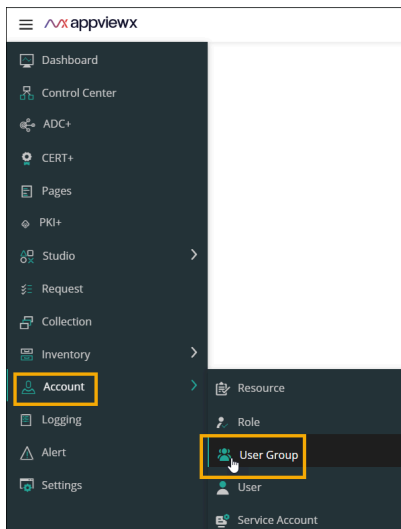
Description

- Click **Submit**.

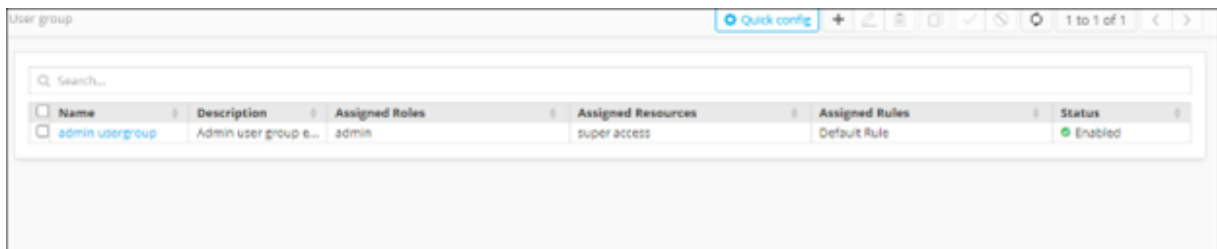
Add New User Group by Bulk Import

To add a new user group using the bulk import feature:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User Group**.



The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.

Navigation: << AUTHENTICATION — USER GROUP — ROLES — RESOURCES

Create User Groups and assign roles. Users assigned to the User Group inherit the roles mapped to the User Group.

Search...

+ Add new group More Actions Refresh 1 to 1 of 1 < >

☐	Name	Assigned Roles	Assigned Resources	Assigned Rules	Status
☐	admin usergro...	admin	super access	Default Rule	Enabled

- Click **+ Add new group**.
- From the **Add user groups** dialog box, select **Bulk import** and click **Proceed**.

Add user groups [X]

☐ Sync groups from LDAP
 ☐ TACACS / RADIUS / SAML / AppViewX
 ☒ Bulk import

Proceed **Cancel**

- Click **Browse**.
- To upload your CSV file, in the **Select a file** field, click **Browse**.



Note: To view the sample file for the formatting of the CSV file, click .

- Click **Upload**. User group validation is performed on the imported user groups and the validation status (Valid/Invalid) is displayed.



Note: The validation status can be invalid for reasons like duplicate group name, invalid group name (group name does not meet the group naming criteria, and so on).

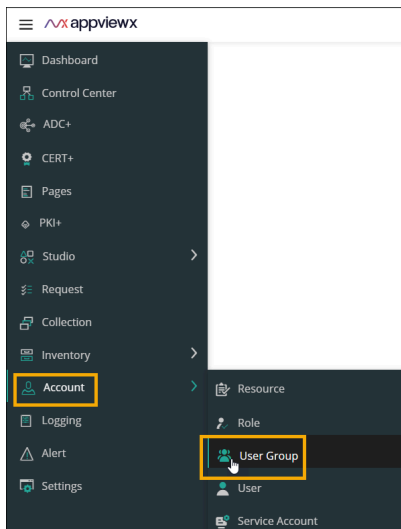
10. To save the user groups, select the list of user groups and click **Submit**.
All user groups with the valid status will be saved into AppViewX.

 **Note:** Once you go back to the User group inventory table, you need to re-upload the file to add the user group.

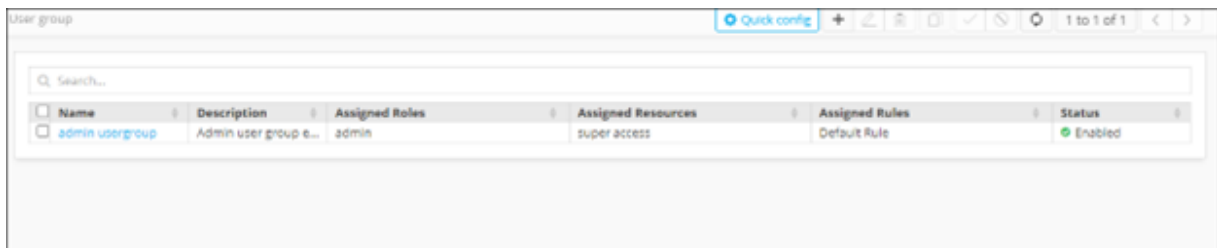
Cloning a User Group

To clone a user group:

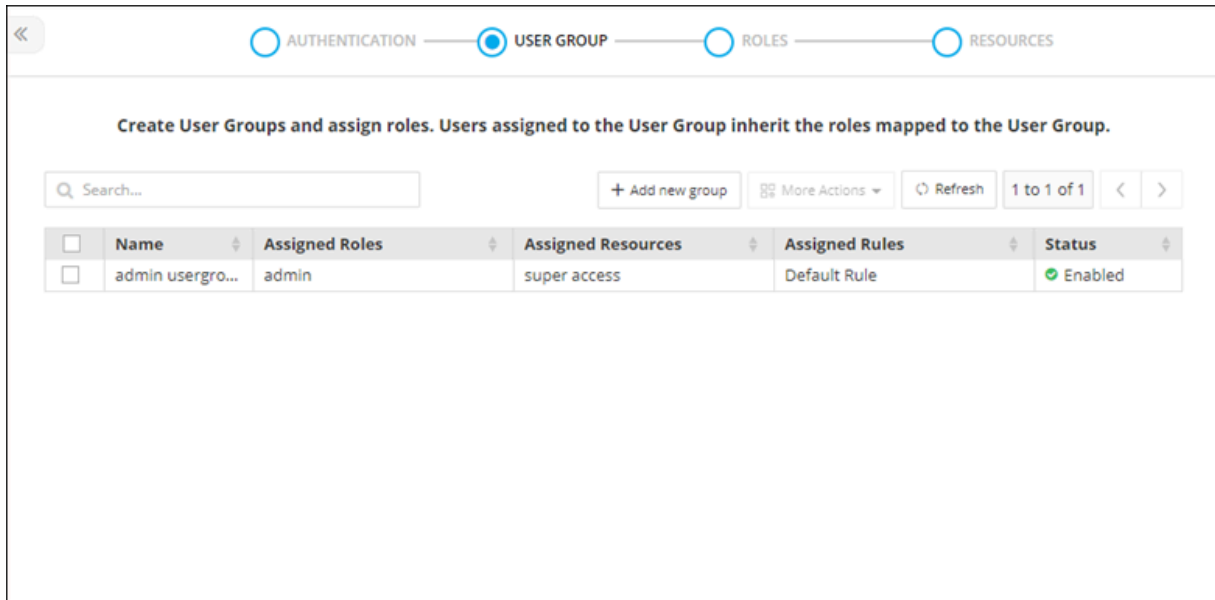
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User Group**.



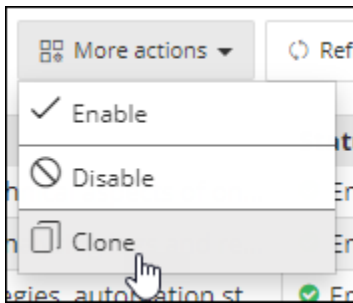
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



- From the inventory table, select the user group to be cloned.
- From the **More Actions** drop-down menu, select **Clone**.

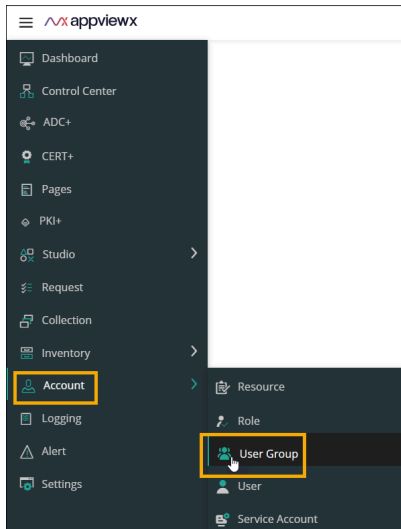


- In the **Clone** dialog box, enter a name for the cloned user group and update the description, if required.
- Click **Save**.

Enabling a User Group

To enable a user group:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Account > User Group**.



The **UserGroup** page is displayed.

User group

Quick config

Search...

Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
admin usergroup	Admin user group e...	admin	super access	Default Rule	Enabled

3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.

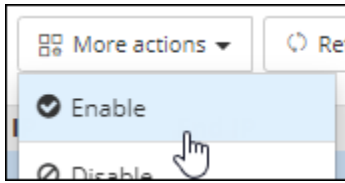
« AUTHENTICATION — USER GROUP — ROLES — RESOURCES

Create User Groups and assign roles. Users assigned to the User Group inherit the roles mapped to the User Group.

Search... + Add new group More Actions Refresh 1 to 1 of 1 < >

Name	Assigned Roles	Assigned Resources	Assigned Rules	Status
admin usergro...	admin	super access	Default Rule	Enabled

- From the inventory table, select the user group to be enabled.
- From the **More Actions** drop-down menu, select **Enable**.

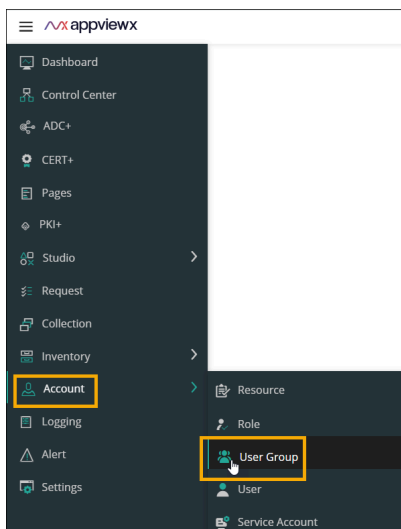


- From the **Enable user group** dialog box, click **Yes**.

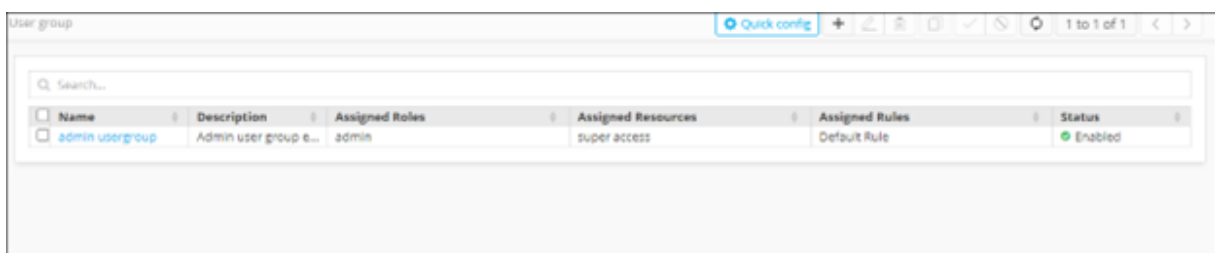
Disabling a User Group

To disable a user group:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Account > User Group**.



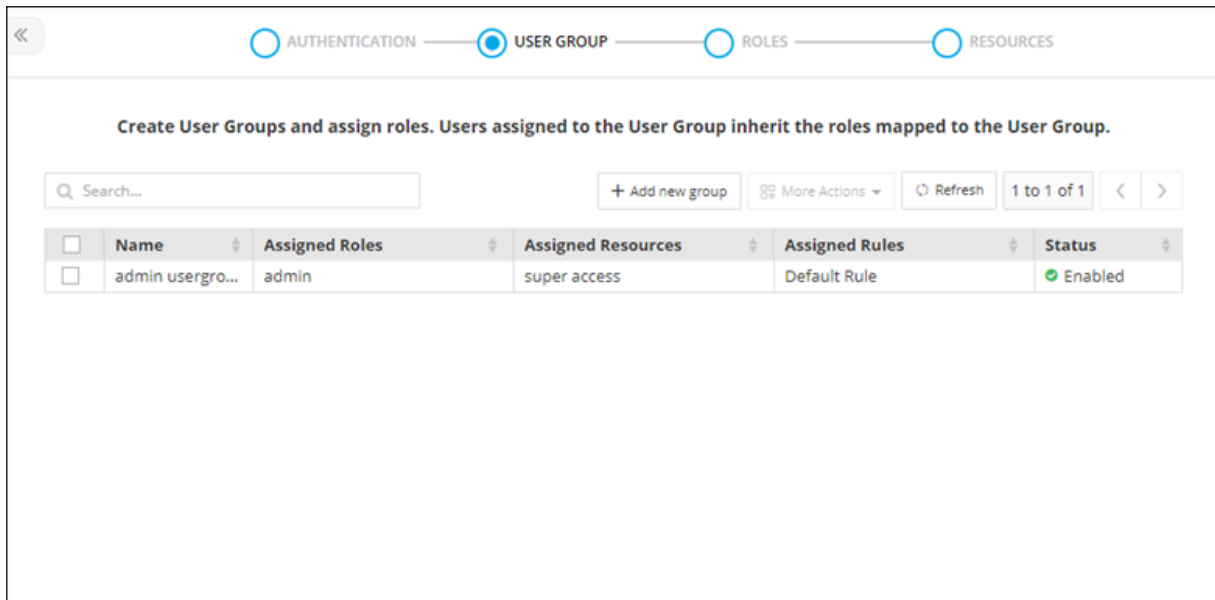
The **UserGroup** page is displayed.



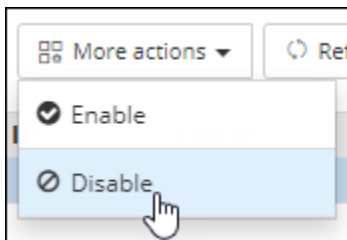
- From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



5. From the inventory table, select the user group to be disabled.
6. From the **More Actions** drop-down menu, select **Disable**.

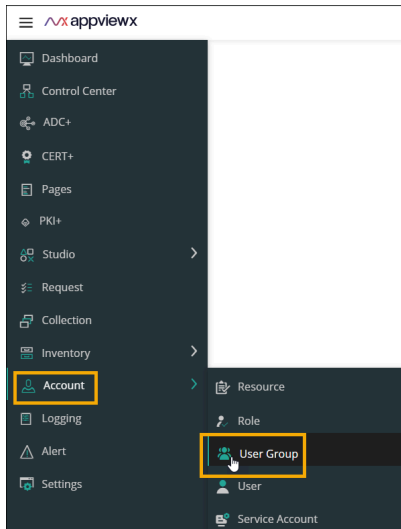


7. From the **Disable user group** dialog box, click **Yes**.

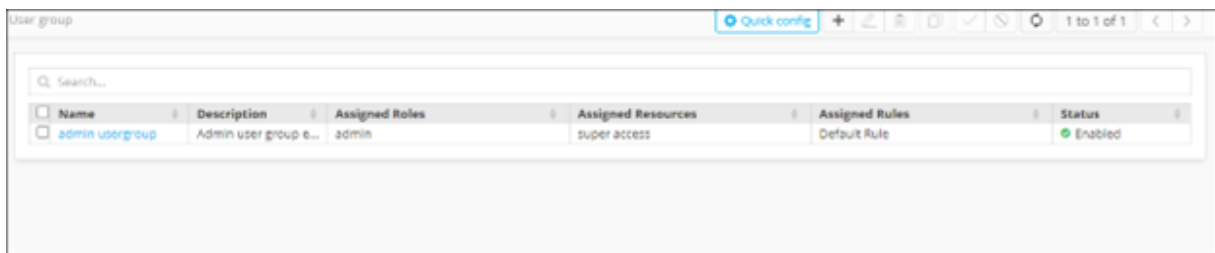
Deleting a User Group

To delete a user group:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Account > User Group**.



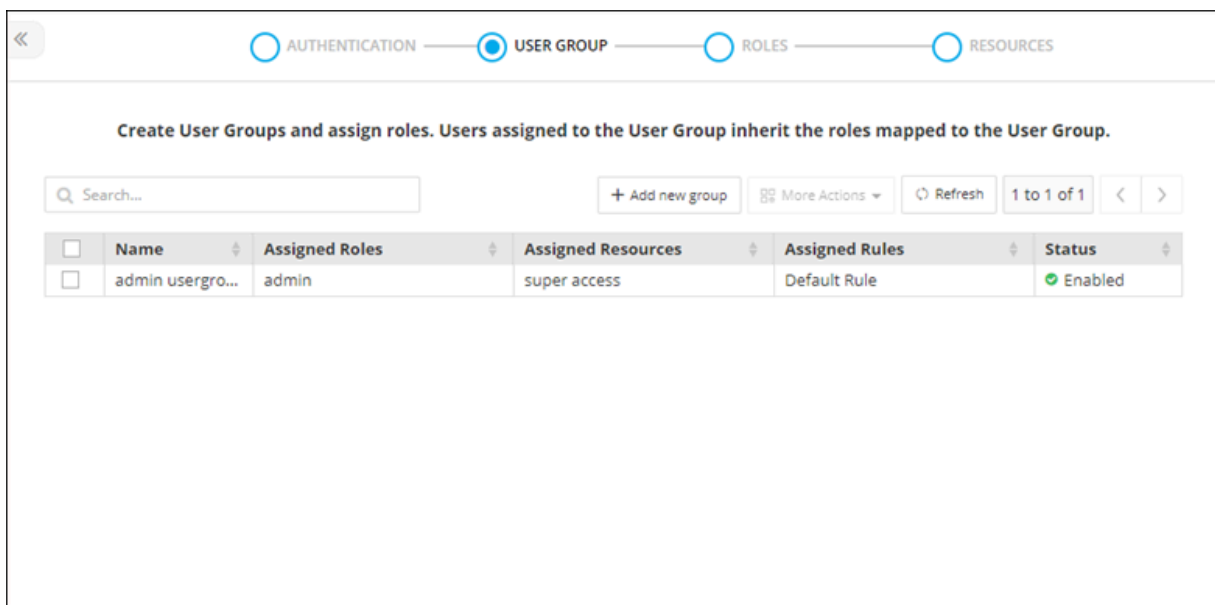
The **UserGroup** page is displayed.



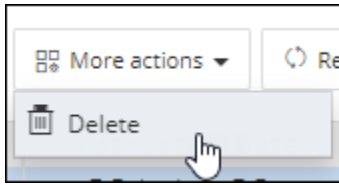
3. From the top-right corner of the screen, click **Quick Config**.

The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



5. From the inventory table, select the user group to be deleted.
6. From the **More Actions** drop-down menu, select **Delete**.



7. From the **Delete user group** dialog box, click **Yes**.

Chapter 4: Configuring Privileged Access Management

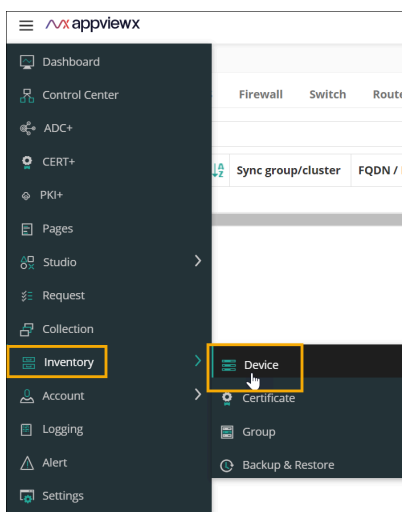
- Overview
- AppViewX
- CyberArk
- Thycotic
- HashiCorp

Overview

For a more sophisticated management of critical data and infrastructure, AppViewX allows for Privileged Access Management (PAM). In simple words, PAM is the practice of managing users/devices/applications that have elevated access to an organization's most confidential and critical resources.

To configure PAM settings:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Inventory > Device**.



The **Device :: ADC** page is displayed.

Device :: ADC

ADC Server WAF DNS Firewall Switch Router Proxy Cloud HSM Others MDM

Search...

Name	Sync group/cluster	FQDN / IP address	Port	Version	Status	Vendor	Modules
15059		192.168.150.56	22	1.5.18	Managed	HAProxy	SLB
192.168.142.197		192.168.142.197	22	13.1.3.4 build 0.0.5	Managed	F5	LTM, BIG-IP DNS
192.168.31.189	hasyncfailover	192.168.31.189	22	15.0.1 build 0.0.11	Managed	F5	LTM, BIG-IP DNS
192.168.31.42		192.168.31.42	22	13.0 build 58.32.nc	Managed	Citrix	SLB
192.168.94.6		192.168.94.6	22	1.8.8	Managed	HAProxy	SLB
aws1234_387848027138			22		Managed	AmazonELB	
gs-f5-pe115.lab.apviewx.net	ha group	192.168.40.169	22	11.6.5.2 build 0.0.10	Managed	F5	LTM, BIG-IP DNS
gs-f5-pe34.apviewx.com	hasyncfailover	192.168.31.188	22	15.0.1 build 0.0.11	Failed	F5	LTM, BIG-IP DNS
test	ha-group	192.168.40.150	22	11.6.5.2 build 0.0.10	Managed	F5	LTM, BIG-IP DNS

3. On the **Device :: ADC** page, click **Credential**.

Device :: ADC

ADC Server DNS Firewall WAF Switch Router Proxy Cloud HSM Others MDM

Search...

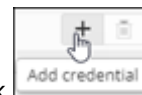
Name	Sync group/cluster	FQDN / IP address	Port	Vendor	Modules	Data center	Object count
No records found							

The **Device > Credential** page is displayed.

Device > Credential

Search...

Credential name	Credential source	Access information	Association status
Default	AppViewX	Username : admin	Passive



4. From the top right corner of this page, to add a credential, click

The **Add Credential** page is displayed.

Device > Credential > Add credential

appviewX

CYBERARK

thycotic

HashiCorp

Credential details

* Credential name

* User name

Credential type ☒ Password ☐ Identity key

* Password

Secondary password

Save Cancel

5. From the left pane, select the vendor for whom you want to configure PAM.
Credential details fields are displayed for the selected vendor.
6. Enter the **Credential details** for the vendor.
 - To enter the credential details for AppViewX, click [here](#).
 - To enter the credential details for CyberArk, click [here](#).
 - To enter the credential details for Thycotic, click [here](#).
 - To enter the credential details for Hashicorp, click [here](#).
7. Click **Save**.

AppViewX

AppViewX is shipped with a built-in integration with HashiCorp Vault for software level security to secure the private keys and device credentials onboarded to the product.

To configure credential details for the AppViewX vault:

1. On the **Add credential** page, in the **Credential details** section, enter the required field information.

Device > Credential > Add credential

Credential details

* Credential name

* User name

Credential type ☒ Password ☐ Identity key

* Password

Secondary password

Save **Cancel**

The following table describes the field information in this section:

Field	Description
*Credential name	Name for the credential for the users to identify it.
*User name	User name used for device onboarding.
Credential type	Select the type of authentication from one of the following: • Password • Identity key
*Password	Password configured at the time of device onboarding.  Note: This field is displayed only when the Credential type is selected as Password.
Secondary password	Additional password enabled by vendors for specific operations.  Note: This field is displayed only when the Credential type is selected as Password.
*Identity key	Credentials (private key in the .pem or .txt format) for enabling device communication via SSH.

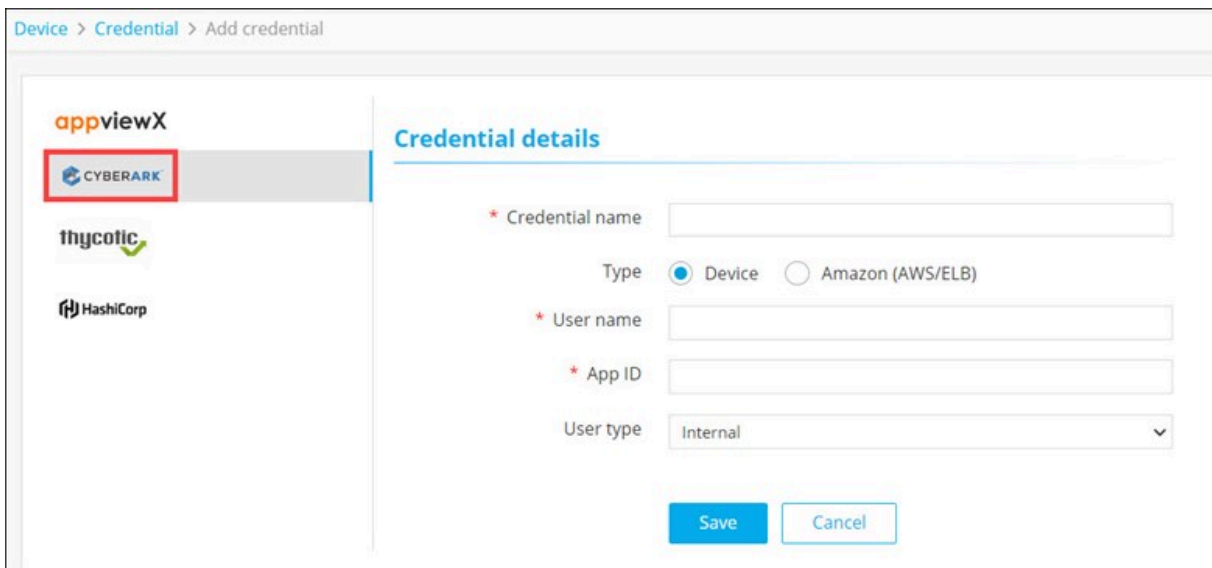
Field	Description
	 Note: This field is displayed only when the Credential type is selected as Identity key .
Passphrase	Key to protect the private key files.  Note: This field is displayed only when the Credential type is selected as Identity key .
All * marked fields are mandatory.	

2. Click **Save**.

CyberArk

To configure credential details for the CyberArk vault:

1. On the **Add credential** page, in the **Credential details** section, enter the required field information.



The following table describes the field information in this section:

Field	Description
*Credential name	Name for the credential for the users to identify it.

Field	Description
Type	To retrieve a credential from the CyberArk vault, select one of the following options: • Device (default) • Amazon (AWS/ELB)  Note: This field is displayed when the Device type is selected.
*User name	User name that has been added in CyberArk.  Note: This field is displayed when the Device type is selected.
*App ID	App ID that has been authorized to provide access to CyberArk and retrieve credentials.  Note: This field is displayed when the Device type is selected.
User type	From the drop-down menu, select one of the following: • Internal (user created directly in the device) • External (user created in the Active Directory)  Note: This field is displayed when the Amazon (AWS/ELB) type is selected.
*AWS IAM username	User name that has been added in CyberArk.  Note: This field is displayed when the Amazon (AWS/ELB) type is selected.
*App ID	Reference ID provided by CyberArk for the corresponding application.  Note: This field is displayed when the Amazon (AWS/ELB) type is selected.
*AWS access key ID	Access key ID generated from the AWS management console.

Field	Description
All * marked fields are mandatory.	

- Click **Save**.

Thycotic

To configure credential details for the Thycotic vault:

- On the **Add credential** page, select **Thycotic** from the left menu.
- In the **Credential details** section, enter the required field information.

The following table describes the field information in this section:

Field	Description
*Credential name	Reference name for Thycotic in AppViewX.
*API Profile	If you have more than one Thycotic Server added as profiles, select the respective profile while adding credentials.
*Secret Type	Select secret type as Device or Amazon.
Username	Enter the username of the secret if you selected the Secret Type as Device.
AWS IAM Username	Enter the AWS IAM username if you selected the Secret Type as Amazon.

Field	Description
All * marked fields are mandatory.	

3. Click **Save**.

• Steps for Integration

Steps for Integration

1. On the **Add credential** page, select **Thycotic** from the left menu.
2. From the top right corner of the page, click **Thycotic API Settings**.

The **Thycotic API Settings** pop-up window is displayed.

API Profile Name*	Hostname/Domain Name	Port	Type	Username	Action
No records found					

The following table describes the field information here:

Field	Description
*API Profile Name	Reference name for the vault in AppViewX.
*Hostname/Domain Name	Enter the Hostname of the Thycotic Secret Server if it is hosted in an on-prem environment or the Domain name of the Thycotic Secret Server if it is the cloud version.
*Port	Port number of the Thycotic Secret Server.
*Type	Select if Thycotic Secret Server is hosted in an On prem or Cloud environment.
*Username	Username of Thycotic Secret Server.

Field	Description
*Password	Password of Thycotic Secret Server.
All * marked fields are mandatory.	



Note: You can add multiple Thycotic Secret Servers as different Profiles. Each Thycotic Secret Server will be added to the Thycotic API settings page.

3. To modify the details of any profiles, click on the name of profile, modify the details and click **Modify**.
4. To delete any profile, click delete icon in Action column of profiles

HashiCorp

To configure credential details for the HashiCorp vault:

1. On the **Add credential** page, in the **Credential details** section, enter the required field information.

The following table describes the field information in this section:

Field	Description
*Credential name	Unique name for the credential for the users to identify it.
*API Profile	Select the API profile from the dropdown list which is configured in HashiCorp API settings.
*Secret Engine	Type path and click enter. It will suggest a list of secrets and the desired secret can be selected.
All * marked fields are mandatory.	

2. Click **Save**.

- [Linking Credentials in AppViewX from Hashicorp Vault](#)

Linking Credentials in AppViewX from Hashicorp Vault

To configure credential details for the HashiCorp vault:

1. On the **Add credential** page, from the top-right corner of the page, click **HashiCorp API Settings**.
The **HashiCorp API Settings** window is displayed.

HashiCorp API Settings

* API Profile Name

* IP / Hostname

* Port

* Vault Token

Add **Reset**

API Profile Name	Hostname	Port	Action
No records found			

The following table describes the field information required here:

Field	Description
*API Profile Name	Enter a unique API profile name.
*IP/Hostname	Enter the HashiCorp vault hosted IP address or hostname.
*Port	Enter the port in which the HashiCorp vault is running.
*Auth Method	From the drop-down list, select either Token/AppRole .

Field	Description
	- If Token is selected, enter the Vault Token for the authentication. Auth Method Token Vault Token - If AppRole is selected, enter the following: Auth Method AppRole Role ID SecretID - Enter the RoleID - Enter the SecretID
Namespace	Enter a namespace.

2. Once the details are entered, click **Add**.



Note: Multiplevaults can be added by configuring multiple profiles.

Chapter 5: Configuring General Settings

- [Configuring the SMTP Settings](#)
- [Managing Proxy Settings](#)
- [Setting the Cryptographic Policy](#)
- [Enabling Dashboard View for the User](#)
- [Managing the Login Configuration](#)

Configuring the SMTP Settings

- [Configuring the SMTP Settings for Google](#)
- [Configuring the SMTP Settings for Microsoft](#)

Configuring the SMTP Settings for Google

The SMTP configuration is required for AppViewX to be able to send logs and alerts via email and for other email related activities such as sending and receiving notifications and so on.

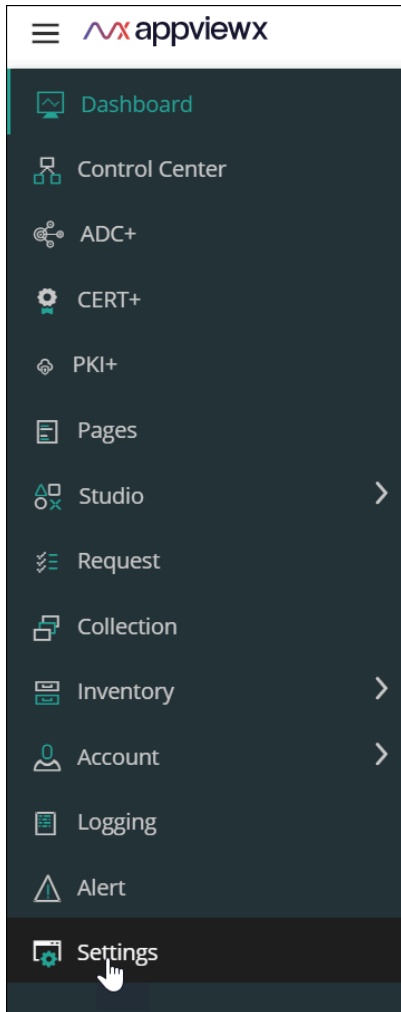
The SMTP oAuth uses an access token instead of a password to send email. The access token works as a temporary password with fixed validity and has permissions delegated by the user.

To get the access token you must provide details such as username, client-id, secret, Authorization endpoint, token Endpoint and scope. Once these details are submitted, you will be redirected to the oAuth server login page. Once the user authorization is done here, the oAuth server returns the Auth code.

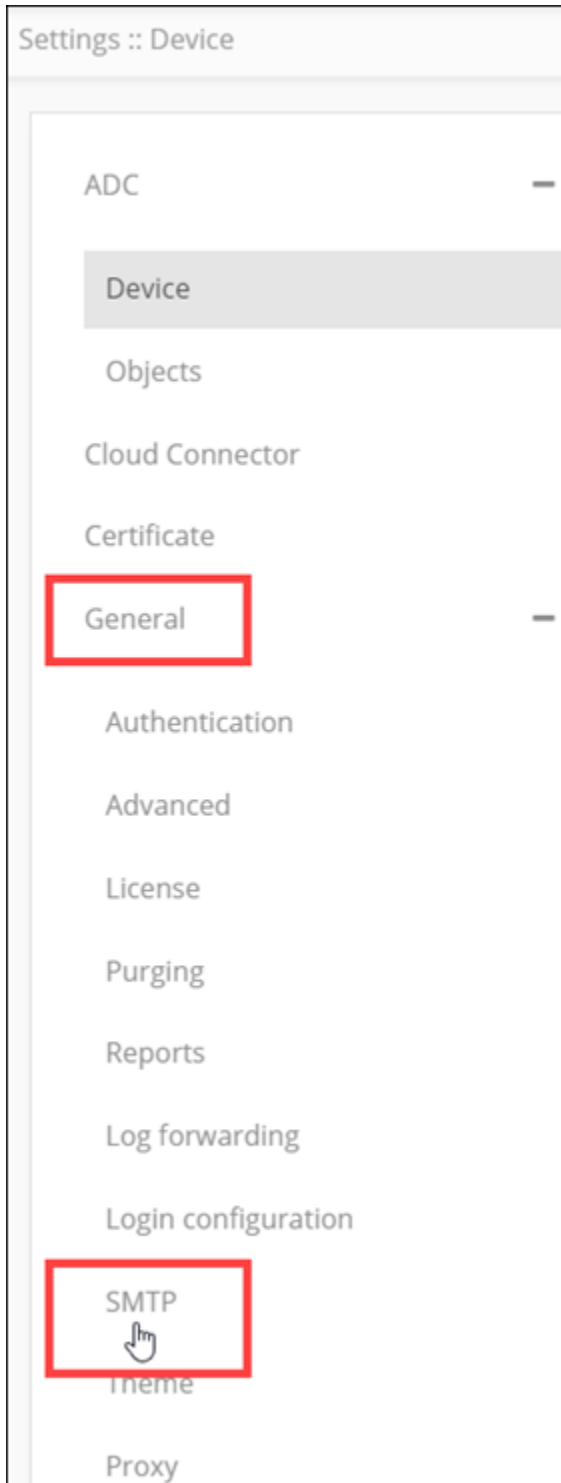
The Auth code is exchanged with the access token and refresh token in the backend and saved in DB.

To configure the SMTP server:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **SMTP**.



The **Settings :: SMTP** page is displayed.

ADC

Device

iHealth report

Objects

Statistics

Backup & Restore

Certificate

General

Authentication

Advanced

License

Purging

Reports

Log forwarding

Login configuration

SMTP

SMTP

SMTP configuration

* SMTP host

smtp.gmail.com

* SMTP port

587

Data center

absecon

* From address

anandkumar.singh@appviewx.com

Enable SSL

☒

* SMTP TLS Version

TLsv1.2

Email box

☐

Authentication

Authentication required

☒

Authentication type

☐ Basic
 ☒ OAuth

* Redirect URL

http://localhost:8000/appviewx/SMTPAuthorize

* Client ID

421727348744-273vgeoch1irt7knrbjev92h40tt70k1.apps.goo

* Client Secret

5. In the **SMTP configuration** section, enter the required field information.

SMTP configuration

*

SMTP host

smtp.gmail.com

*

SMTP port

587

Data center

absecon

▼

*

From address

anandkumar.singh@appviewx.com

Enable SSL

☒

*

SMTP TLS Version

TLV1.2

▼

i

Email box

☐

i

The following table describes the fields in this section:

Field	Description
*SMTP host	Host name of the SMTP server.
*SMTP port	Port number of the SMTP server.
Data center	From the options available in the dropdown, select the data center.
*From address	Enter the email address that will be used to email the logs and alerts.
Enable SSL	To allow SSL encryption, enable this toggle key.
*SMTP TLS Version	From the options available in the dropdown, select the TLS version of the SMTP server.  Note: Versions 1.2 and higher are recommended.
Email box	To use the mailbox feature to read emails in Visual Workflow, enable this toggle key.
*Email	Email address of the IMAP server used for the mailbox feature.

Field	Description
	 Note: This field is displayed only if the Email box key is enabled.
*Password	Password of the IMAP server used for the mailbox feature.  Note: This field is displayed only if the Email box key is enabled.
*Host name	Host name of the IMAP server used for the mailbox feature.  Note: This field is displayed only if the Email box key is enabled.
*Port	Enter the Port number.  Note: This field is displayed only if the Email box key is enabled.
All * marked fields are mandatory.	

6. In the **Authentication** section, enter the required field information.

Authentication

Authentication required ☒

Authentication type ☐ Basic ☒ OAuth

* Redirect URL

* Client ID

* Client Secret

* Authorization endpoint

* Token endpoint

* Scope

* Username

This table describes the fields in this section:

Field	Description
Authentication required	To enable authenticated mail server communication, enable this toggle.
Authentication type	Select the Authentication type as Basic.  Note: Selecting Basic displays the Username and Password fields. Select the Authentication type as OAuth.  Note: Selecting OAuth displays the fields that are described below.
*Redirect URL	This field is auto-populated from the address bar of the browser.
*Client ID	Enter the Client ID that is generated in the OAuth server when the OAuth client is created.

Field	Description
	 Note: The steps to create an oAuth client are different for Google and Microsoft. For more information on steps for Google, click here. For more information on steps for Microsoft click here.
*Client Secret	Enter the Client Secret that is generated in the oAuth server when the oAuth client is created.
*Authorization endpoint	Enter the authorization endpoint where the user authorizes and gives permission to the oAuth client to send email on behalf of the user.
*Token endpoint	Enter the token endpoint to get Access Token and Refresh Token. You can get the endpoint by providing Client ID, Secret, and other relevant values based on oAuth 2.0 specifications.
*Scope	The permission required to send email.  Note: For Google, enter https://mail.google.com/.
*Username	 Note: This field is enabled only if the Authentication required key is enabled. Username for the authenticated mail server
*Password	 Note: This field is enabled if you select Basic as your Authentication type. Authentication Authentication required ☒ Authentication type ☒ Basic ☐ oAuth * Username * Password Enter the valid password associated with the username.
All * marked fields are mandatory.	

7. In the **Test email** section, enter the email address to which a test email should be sent and click **Test**.
8. To save the SMTP configuration settings, click **Save & Authorize**.
9. Displays confirmation of SMTP Settings Authorized.

A new tab opens asking for sign-in.

Once authorization is done the user receives an Access Token and a Refresh Token from the Token endpoint. The Access token is used for sending email and the Refresh token is used for renewing the Access token upon its expiry.

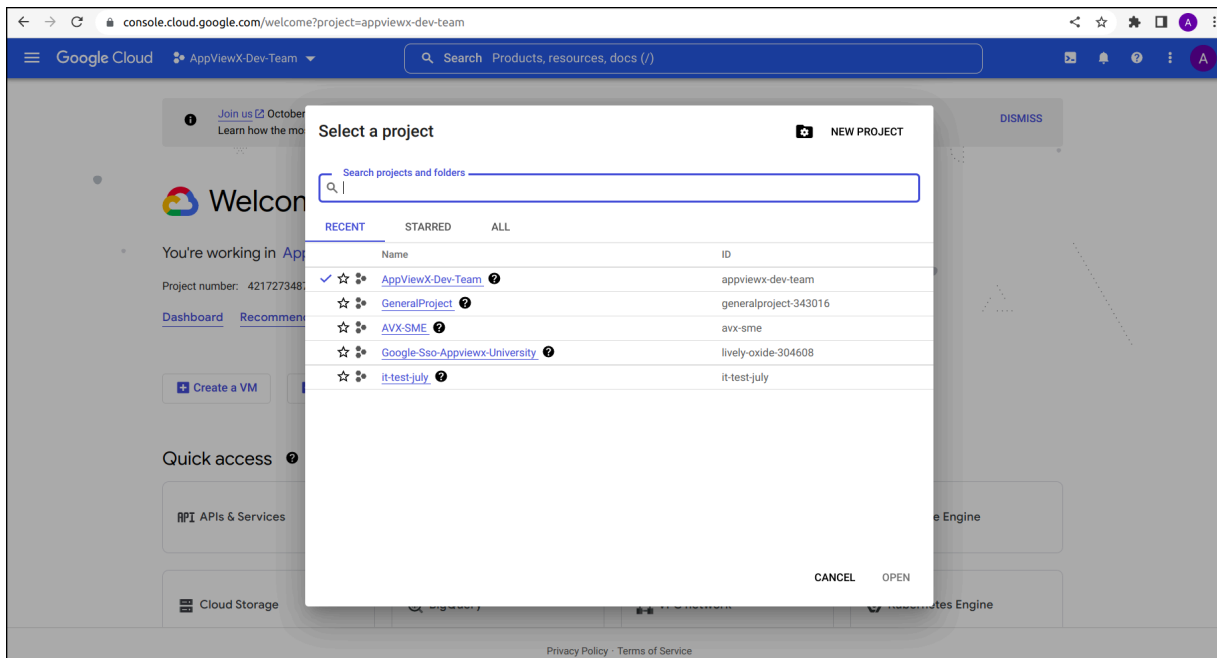
• Authentication for Google SMTP Settings

Authentication for Google SMTP Settings

Create authorization credentials

Any application that uses OAuth 2.0 to access Google APIs must have authorization credentials that identify the application to Google's OAuth 2.0 server. The following steps explain how to create credentials for your project. Your applications can then use the credentials to access APIs that you have enabled for that project.

1. Google **App Registration** URL: <https://console.cloud.google.com/>.



2. From the project drop-down, select an existing project, or create a new one by clicking on **NEW PROJECT**.
3. In the sidebar hover the mouse pointer over the "APIs & Services", click **OAuth consent screen**.

The **OAuth consent screen:: App information** page is displayed.

← → ↻ console.cloud.google.com/apis/credentials/consent/edit?project=appviewx-dev-team

Google Cloud AppViewX-Dev-Team Search Products, resources, docs (/)

APIs & Services Edit app registration

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *
SMTP-TEST
The name of the app asking for consent

User support email *
cloud@appviewx.com
For users to contact you with questions about their consent

App logo [BROWSE](#)
Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page
Provide users a link to your home page

Application privacy policy link
Provide users a link to your public privacy policy

Application terms of service link
Provide users a link to your public terms of service

Page usage agreements

Application terms of service link
Provide users a link to your public terms of service

Authorized domains ⓘ

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

Authorized domain 1 *
appviewx.net

Authorized domain 2 *
appvx.com

[+ ADD DOMAIN](#)

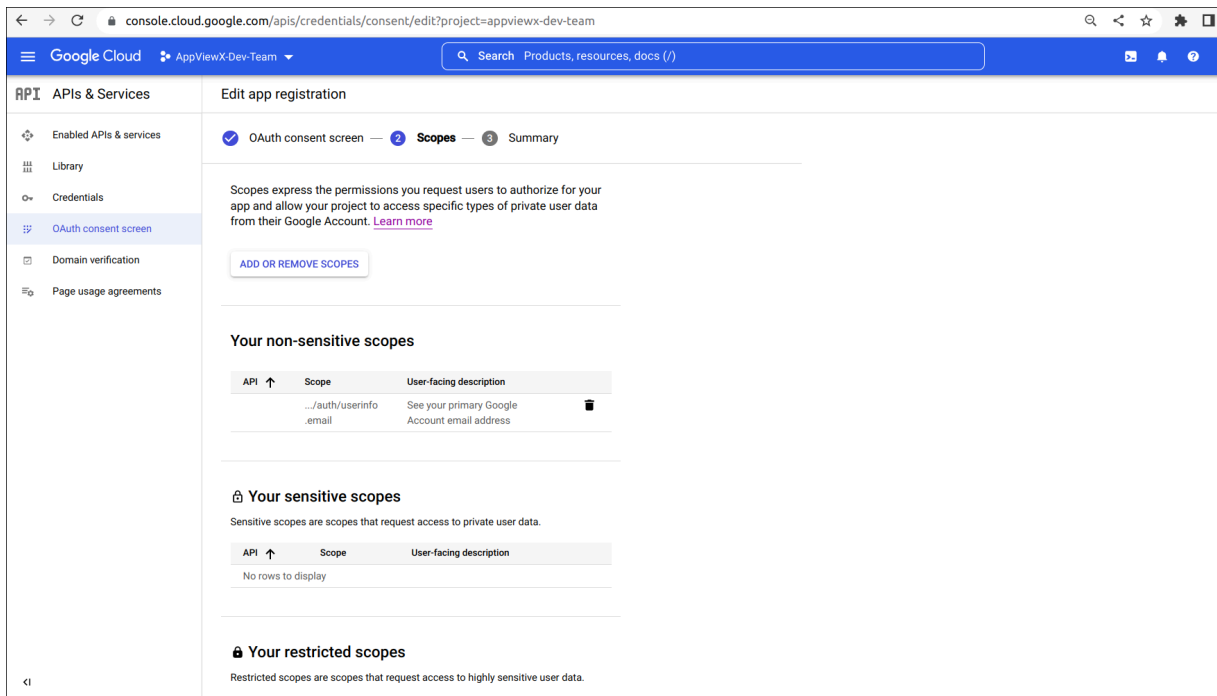
Developer contact information

Email addresses *
developer-testing@appviewx.com ⓘ
These email addresses are for Google to notify you about any changes to your project.

[SAVE AND CONTINUE](#) [CANCEL](#)

- In the **App information** section, enter the required field information. **App name***, **User support email***, **Authorized domains**, and **Developer contact information**, then click **Save & Continue**.

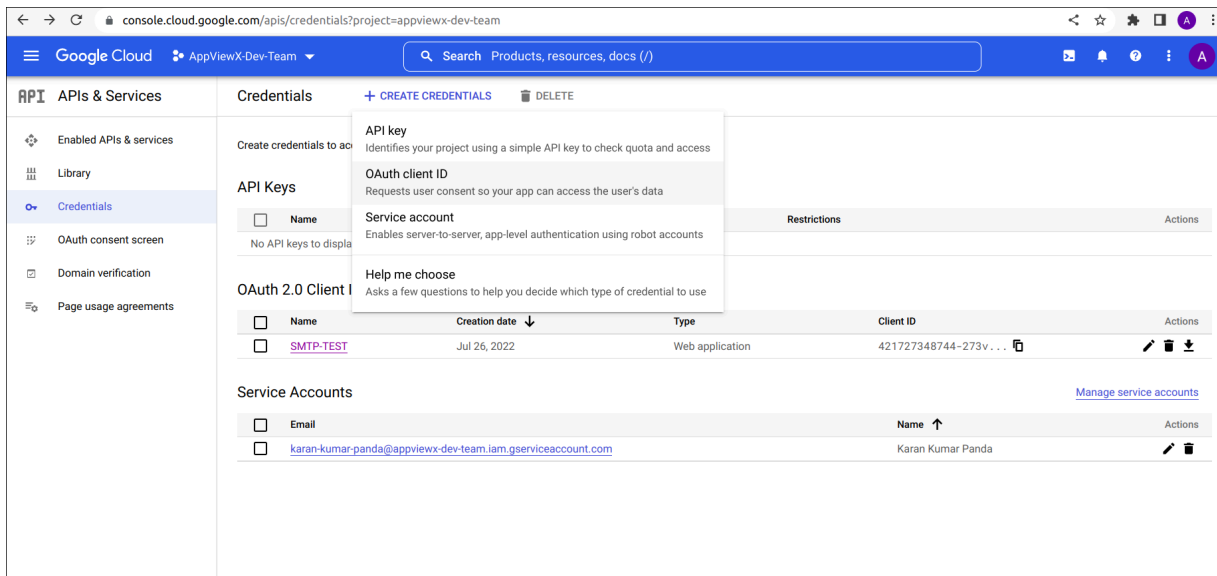
The **Save & Continue :: Scopes** page is displayed.



5. Under **Scopes** section, **ADD SCOPES** required information.

6. In the sidebar hover the mouse pointer over the "APIs & Services", click **Credentials**.

The **APIs & Services :: Credentials** page is displayed.

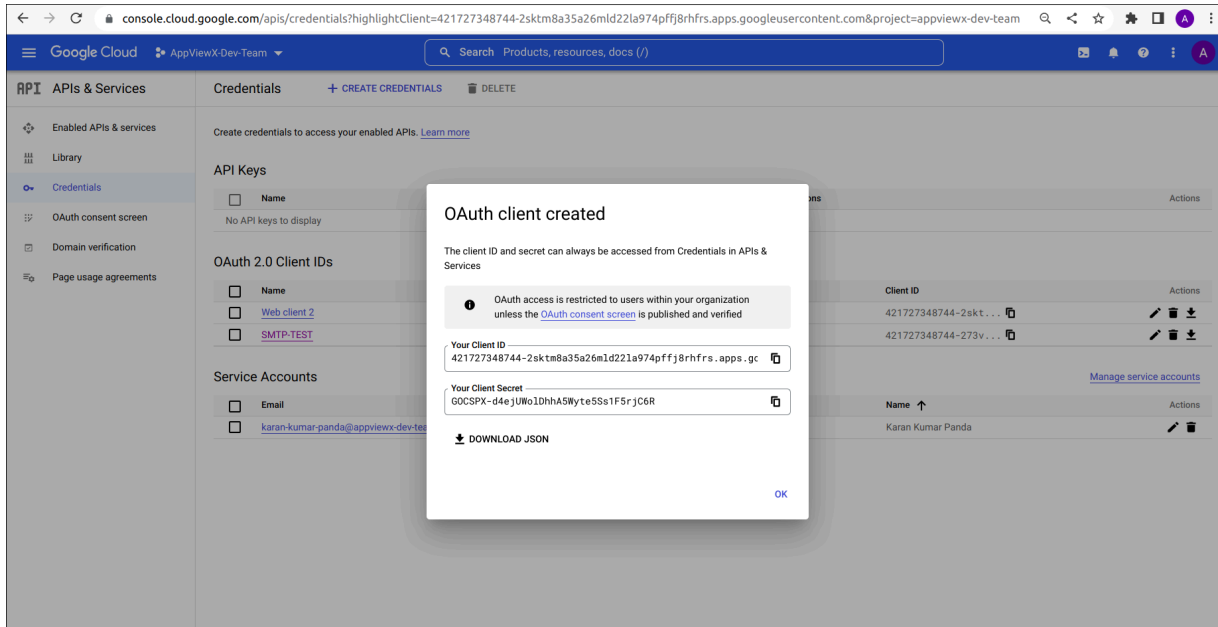


7. In the **Credentials** tab, click the **+CREATE CREDENTIALS**, from the drop-down list, choose **OAuth client ID**.

The **+CREATE CREDENTIALS :: Create OAuth client ID** page is displayed.

The screenshot shows the 'Create OAuth client ID' page in the Google Cloud console. The left sidebar is titled 'APIs & Services' and has 'Credentials' selected. The main content area is titled 'Create OAuth client ID'. It contains a description of a client ID, a form for 'Application type' (set to 'Web application') and 'Name' (set to 'Web client 2'), and a section for 'Authorized redirect URIs' with one URI added: 'https://saas-final-fp-new-02.qa.appvx.com/appviewx/SMTPAuthorize'. There are also sections for 'Authorized JavaScript origins' and 'Authorized redirect URIs' with '+ ADD URI' buttons.

8. Enter the required field information, for **Application type*** select **Web application** and specify **Name*** then click **Save**.
9. Displays confirmation of **OAuth client Created**, with Your Client ID and Your Client Secret.



10. Copy the **Client ID** and **Client Secret** for Authentication of SMTP Server Settings.
11. Authorization endpoint URL: <https://accounts.google.com/o/oauth2/v2/auth>.
12. Token endpoint URL: <https://oauth2.googleapis.com/token>.

Configuring the SMTP Settings for Microsoft

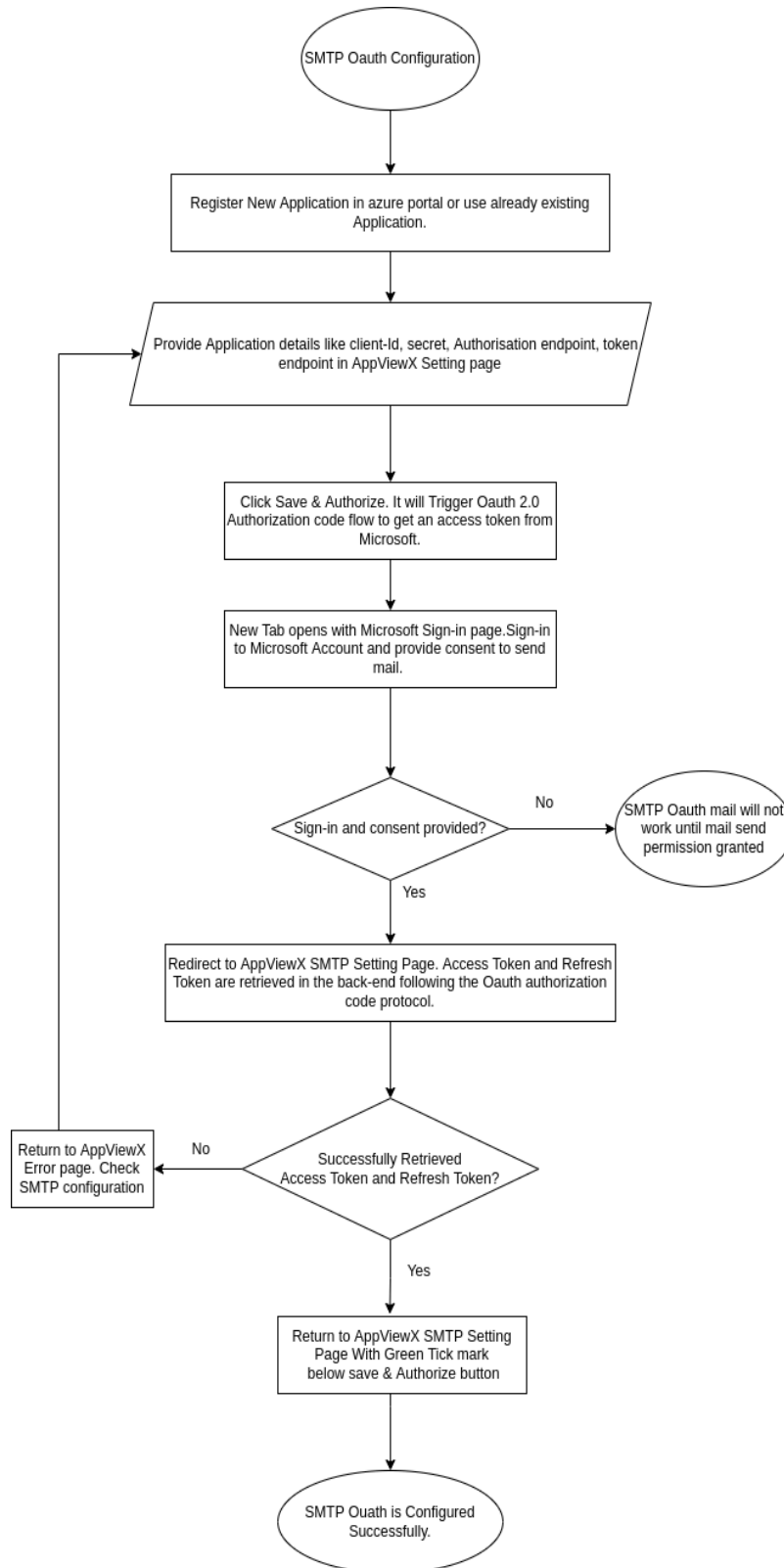
The SMTP configuration is required for AppViewX to be able to send logs and alerts via email and for other email related activities such as sending and receiving notifications and so on.

The SMTP OAuth uses an access token instead of a password to send email. The access token works as a temporary password with fixed validity and has permissions delegated by the user.

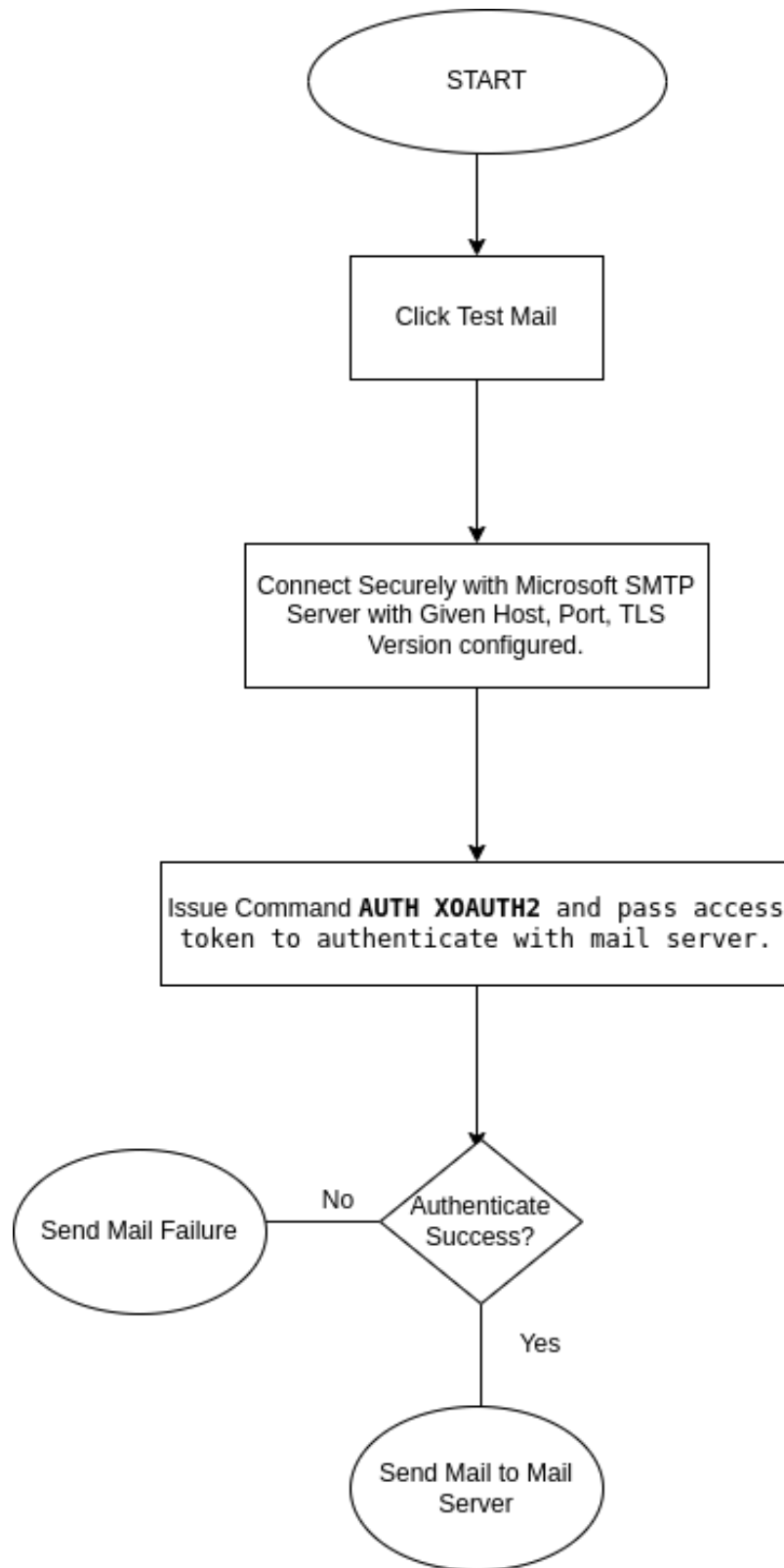
To get the access token you must provide details such as username, client-id, secret, Authorization endpoint, token Endpoint and scope. Once these details are submitted, you will be redirected to the OAuth server login page. Once the user authorization is done here, the OAuth server returns the Auth code.

The Auth code is exchanged with the access token and refresh token in the backend and saved in DB.

Flow Chart for SMTP OAuth Configuration.

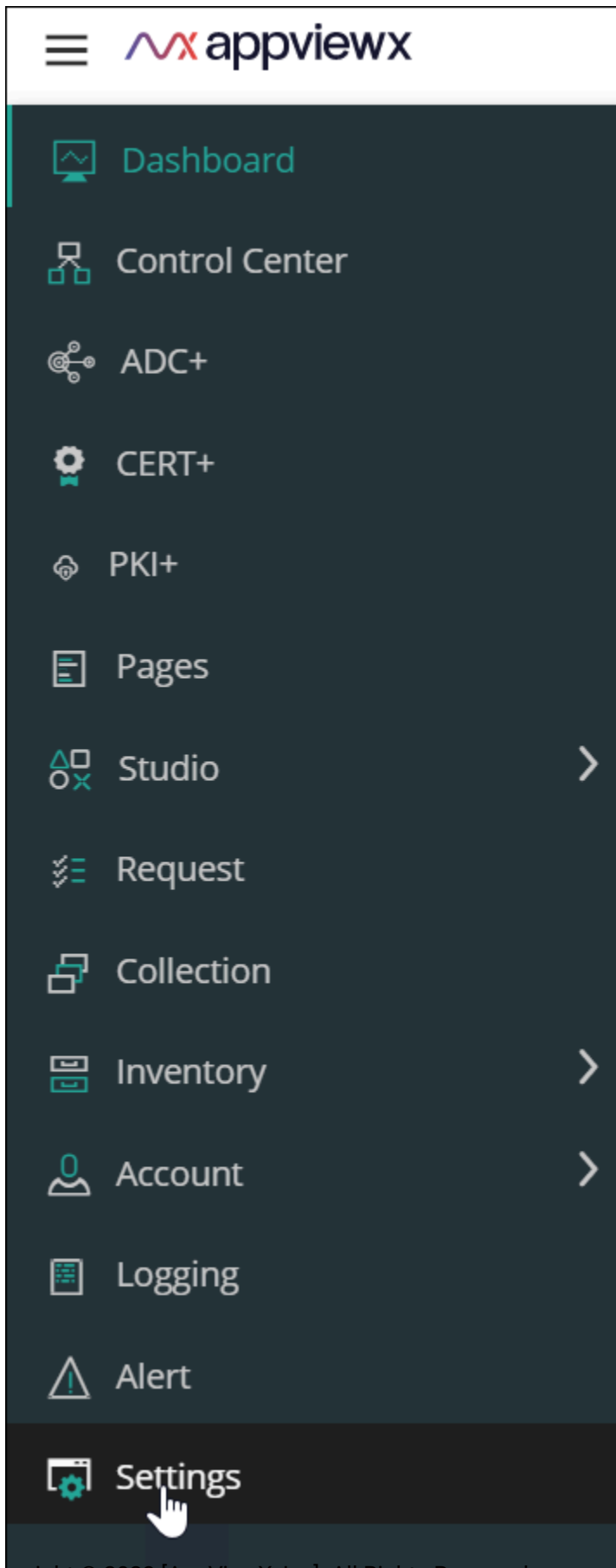


Flow Chart for Test Mail.

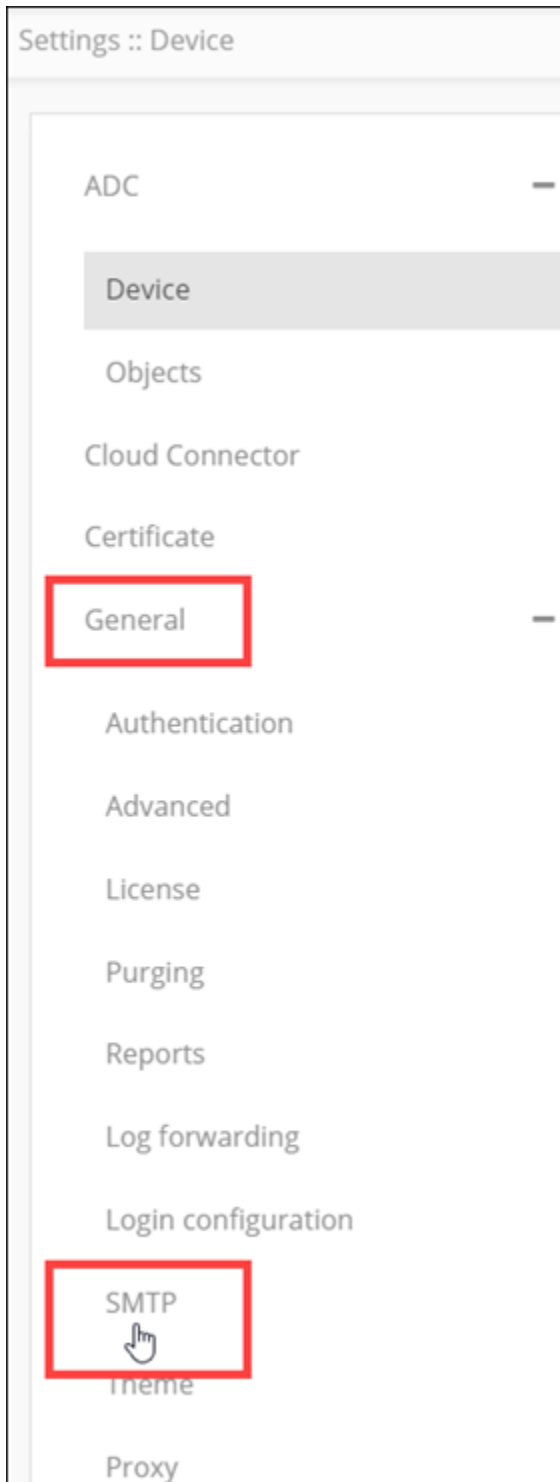


To configure the SMTP server:

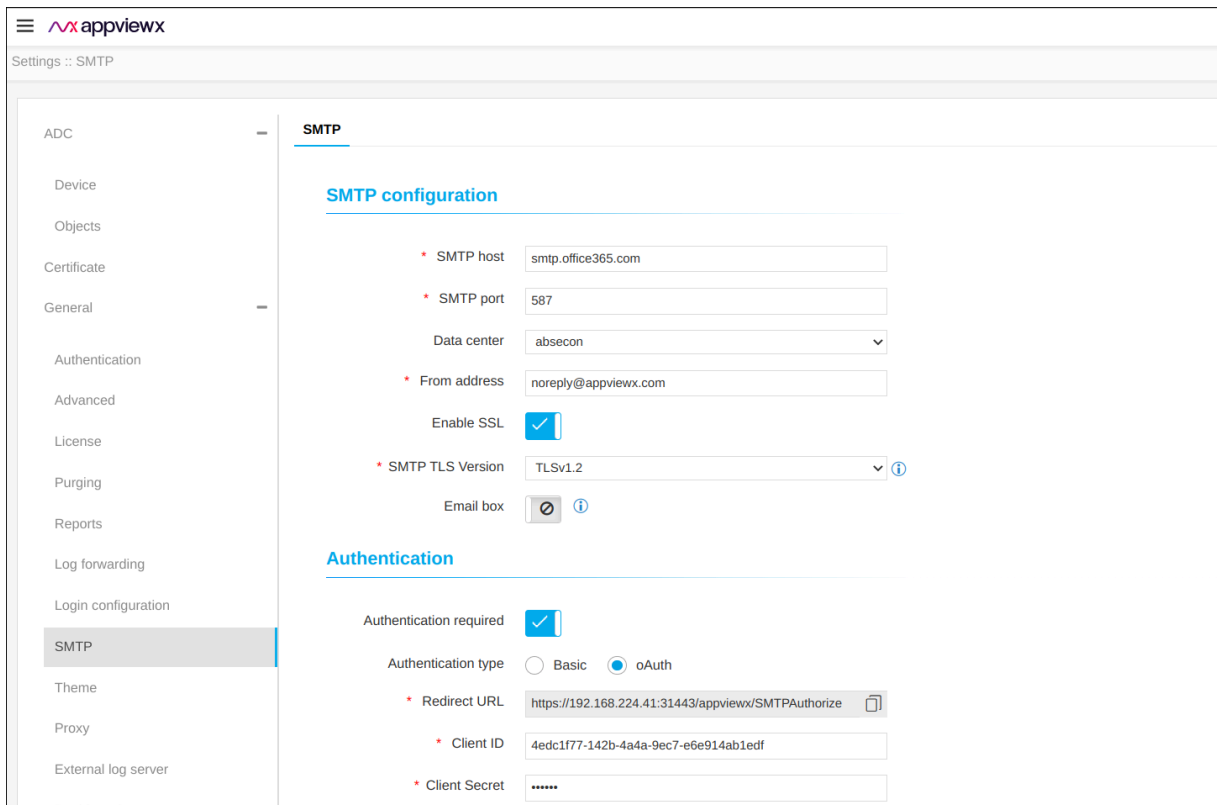
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **SMTP**.



The **Settings :: SMTP** page is displayed.



Settings :: SMTP

ADC

Device

Objects

Certificate

General

Authentication

Advanced

License

Purging

Reports

Log forwarding

Login configuration

SMTP

Theme

Proxy

External log server

SMTP configuration

* SMTP host

* SMTP port

Data center

* From address

Enable SSL ☒

* SMTP TLS Version

Email box ☐

Authentication

Authentication required ☒

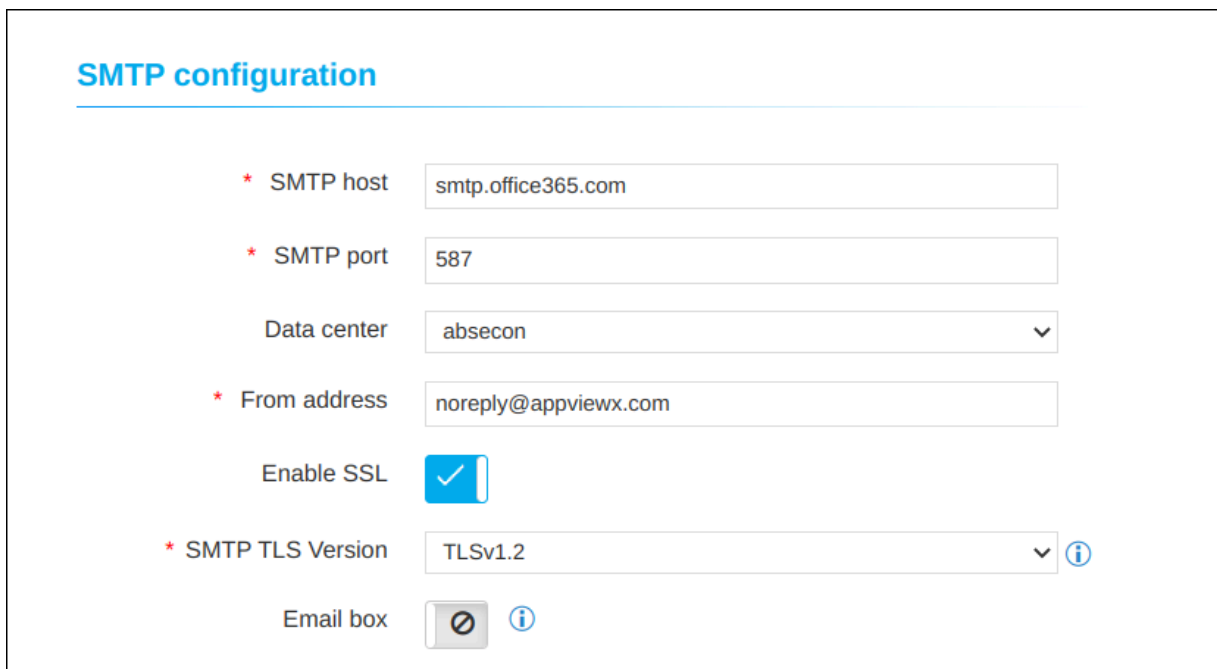
Authentication type ☐ Basic ☒ OAuth

* Redirect URL

* Client ID

* Client Secret

5. In the **SMTP configuration** section, enter the required field information.



SMTP configuration

* SMTP host

* SMTP port

Data center

* From address

Enable SSL ☒

* SMTP TLS Version

Email box ☐

The following table describes the fields in this section:

Field	Description
*SMTP host	Host name of the SMTP server.
*SMTP port	Port number of the SMTP server.
Data center	From the options available in the dropdown, select the data center.
*From address	Enter the email address that will be used to email the logs and alerts.
Enable SSL	To allow SSL encryption, enable this toggle key.
*SMTP TLS Version	From the options available in the dropdown, select the TLS version of the SMTP server.  Note: Versions 1.2 and higher are recommended.
Email box	To use the mailbox feature to read emails in Visual Workflow, enable this toggle key.
*Email	Email address of the IMAP server used for the mailbox feature.  Note: This field is displayed only if the Email box key is enabled.
*Password	Password of the IMAP server used for the mailbox feature.  Note: This field is displayed only if the Email box key is enabled.
*Host name	Host name of the IMAP server used for the mailbox feature.  Note: This field is displayed only if the Email box key is enabled.
*Port	Enter the Port number.  Note: This field is displayed only if the Email box key is enabled.
All * marked fields are mandatory.	

6. In the **Authentication** section, enter the required field information.

Authentication

Authentication required
☒

Authentication type
☐ Basic
☒ OAuth

* Redirect URL

* Client ID

* Client Secret

* Authorization endpoint

* Token endpoint

* Scope

* Username

This table describes the fields in this section:

Field	Description
Authentication required	To enable authenticated mail server communication, enable this toggle.
Authentication type	Select the Authentication type as Basic.  Note: Selecting Basic displays the Username and Password fields. Select the Authentication type as OAuth.  Note: Selecting OAuth displays the fields that are described below.

Field	Description
	SMTP OAuth method to send email, we can't use a different address in From field. The sending address must be the same with the authenticated account.
*Redirect URL	This field is auto-populated from the address bar of the browser.
*Client ID	Enter the Client ID that is generated in the OAuth server when the OAuth client is created.  Note: The steps to create an OAuth client are different for Google and Microsoft. For more information on steps for Google, click here. For more information on steps for Microsoft click here.
*Client Secret	Enter the Client Secret that is generated in the OAuth server when the OAuth client is created.
*Authorization endpoint	Enter the authorization endpoint where the user authorizes and gives permission to the OAuth client to send email on behalf of the user.
*Token endpoint	Enter the token endpoint to get Access Token and Refresh Token. You can get the endpoint by providing Client ID, Secret, and other relevant values based on OAuth 2.0 specifications.
*Scope	The permission required to send email.  Note: For Microsoft, enter https://outlook.office.com/SMTP.Send.
*Username	 Note: This field is enabled only if the Authentication required key is enabled. Username for the authenticated mail server If the Authentication is chosen as OAuth the Username and From address should be the same.

Field	Description
*Password	 Note: This field is enabled if you select Basic as your Authentication type. Authentication Authentication required ☒ Authentication type ☒ Basic ☐ oAuth * Username * Password Enter the valid password associated with the username.
All * marked fields are mandatory.	

- In the **Test email** section, enter the email address to which a test email should be sent and click **Test**.
- To save the SMTP configuration settings, click **Save & Authorize**.
- New Tab is opened for Single Sign On (SSO) with microsoft.
- Provide your login credentials and submit your consent for the mentioned permissions. The login credential should be the same as the username configured in the SMTP Authentication.

11. Displays confirmation of SMTP Settings Authorized.

Settings :: SMTP

Purging

Reports

Log forwarding

Login configuration

SMTP

Theme

Proxy

External log server

Dashboard

Provisioning

SSH

Firewall

Integration

Email box  

Authentication

Authentication required ☒

Authentication type ☐ Basic ☒ OAuth

* Redirect URL 

* Client ID

* Client Secret

* Authorization endpoint

* Token endpoint

* Scope

* Username

 Your settings is authorized

12. AppViewX can send an Email on behalf of the authorized user as the user has given the consent to send Email on his behalf during Authentication.

A new tab opens asking for sign-in.

Once authorization is done the user receives an Access Token and a Refresh Token from the Token endpoint. The Access token is used for sending email and the Refresh token is used for renewing the Access token upon its expiry.

- [Authentication for Microsoft SMTP Settings](#)
- [Frequently Asked Questions](#)

Authentication for Microsoft SMTP Settings

Create authorization credentials

Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around.

Follow these steps to create the app registration:

1. Microsoft App Registration URL: <https://portal.azure.com/>.
2. Under **Manage**, click **App registrations** > **New registration**.

The screenshot shows the 'App registrations' page in the Microsoft Azure portal. The page has a navigation bar with 'New registration', 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', 'Preview features', and 'Got feedback?'. Below the navigation bar, there's a 'New registration' button and a notification banner about feature updates. The main section is titled 'App registrations' and shows a list of 9 applications found. The table below lists the applications with their display names, application (client) IDs, creation dates, and certificate status.

Display name	Application (client) ID	Created on	Certificates & secrets
AppviewxQANODE	2c15ad4b-f01f-4355-a9cf-dca82512b94f	9/2/2022	Current
latest	e0fd37cf-c474-4f98-bb52-d35108269d5f	9/2/2022	Current
newwww	dad81196-c2f4-46f9-b41e-b318487495c6	9/1/2022	Current
QANODE	6308463e-453a-4956-9382-a31c52152ad5	9/1/2022	Current
QANODE	f65fa749-3614-46ba-bb2c-49e0d206bafd	9/1/2022	-
SMTP-TEST	5fd11a2d-d515-4512-9e17-b9201dcc8b31	8/24/2022	Current
TEST	4edc1f77-142b-4a4a-9ec7-e6e914ab1edf	9/1/2022	Current
TEST-SMTP	7401488a-9caa-4fe2-acaa-1f65252772a2	9/12/2022	Current

3. In the **Register an Application** section, enter the required field information.

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page has a navigation bar with 'Name', 'Supported account types', 'Redirect URI (optional)', and 'Register'. The 'Name' section has a text input field for the user-facing display name. The 'Supported account types' section has radio buttons for different account types. The 'Redirect URI (optional)' section has a dropdown for 'Select a platform' and a text input for the URI. The 'Register' button is at the bottom.

Name
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (AppViewX Private Limited only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only
[Help me choose...](#)

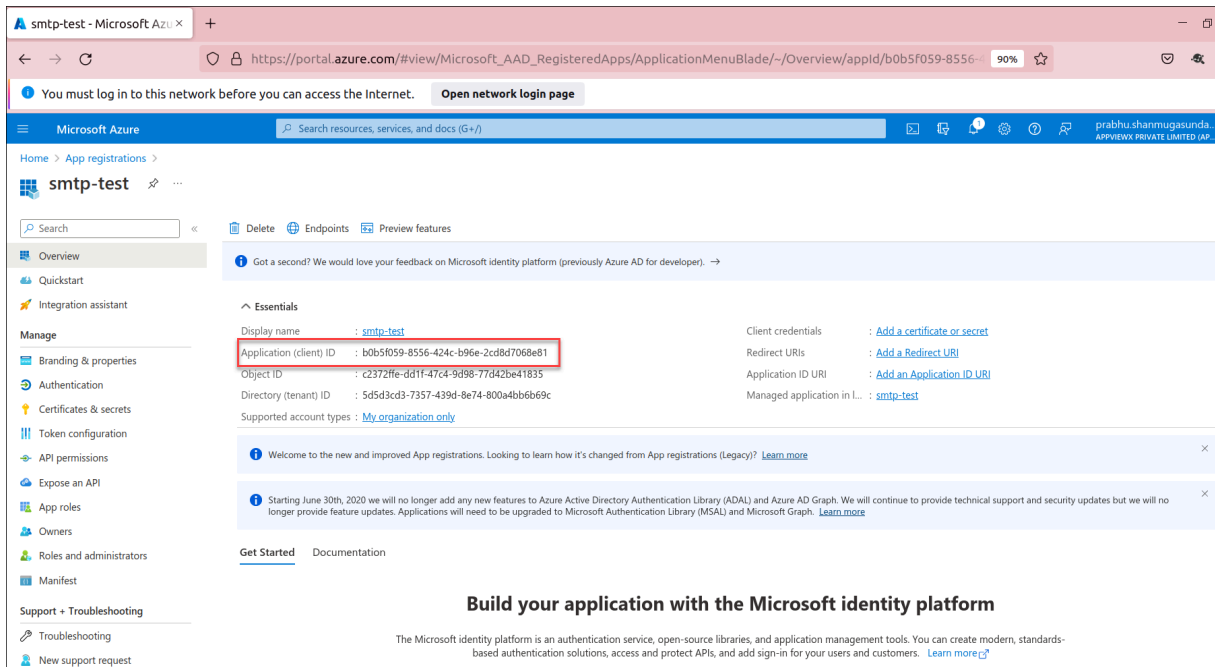
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Select a platform:

By proceeding, you agree to the Microsoft Platform Policies [Go to](#)

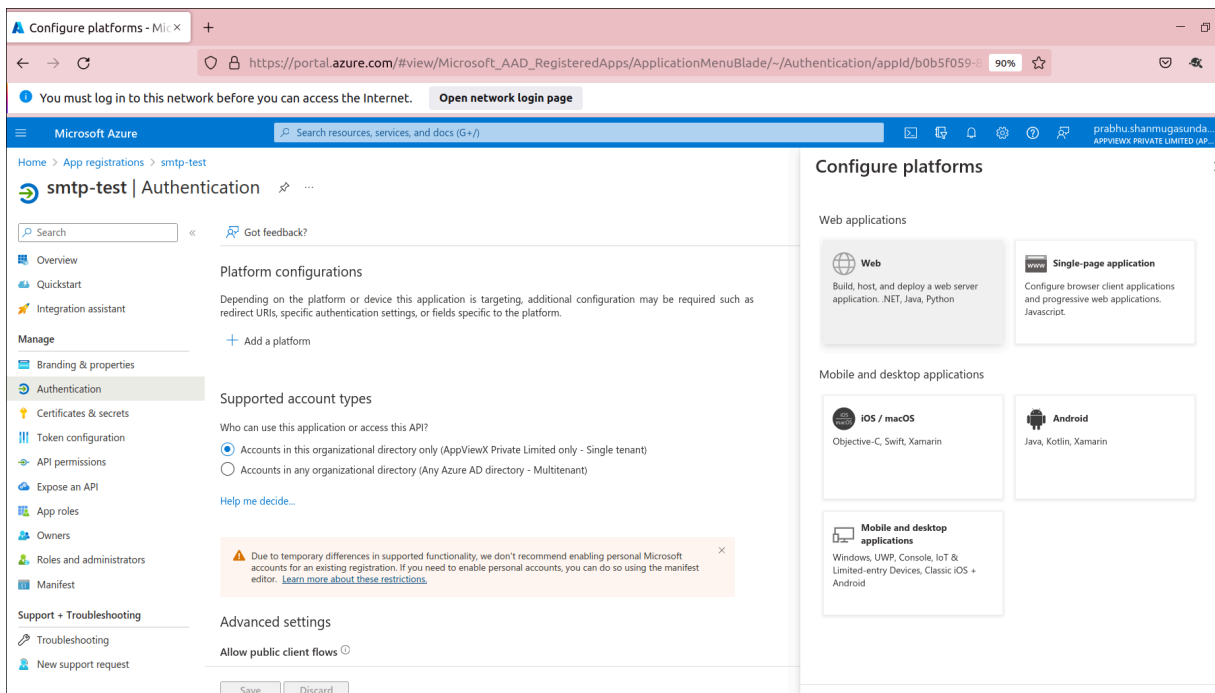
Register

4. Click **Register** to complete the initial app registration.

5. When registration finishes, the Azure portal displays the app registration's Overview pane. You see the **Application (client) ID**.

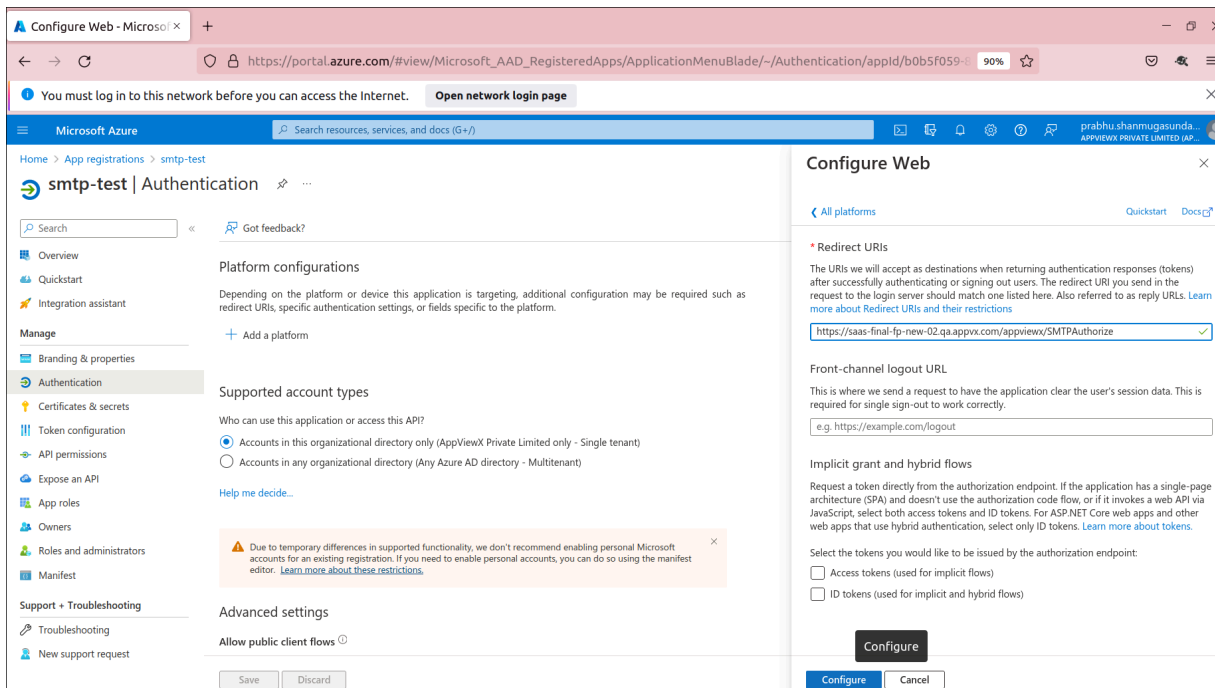


6. Under **Manage**, select **Authentication**.
7. Under **Platform configurations**, select **Add a platform**.

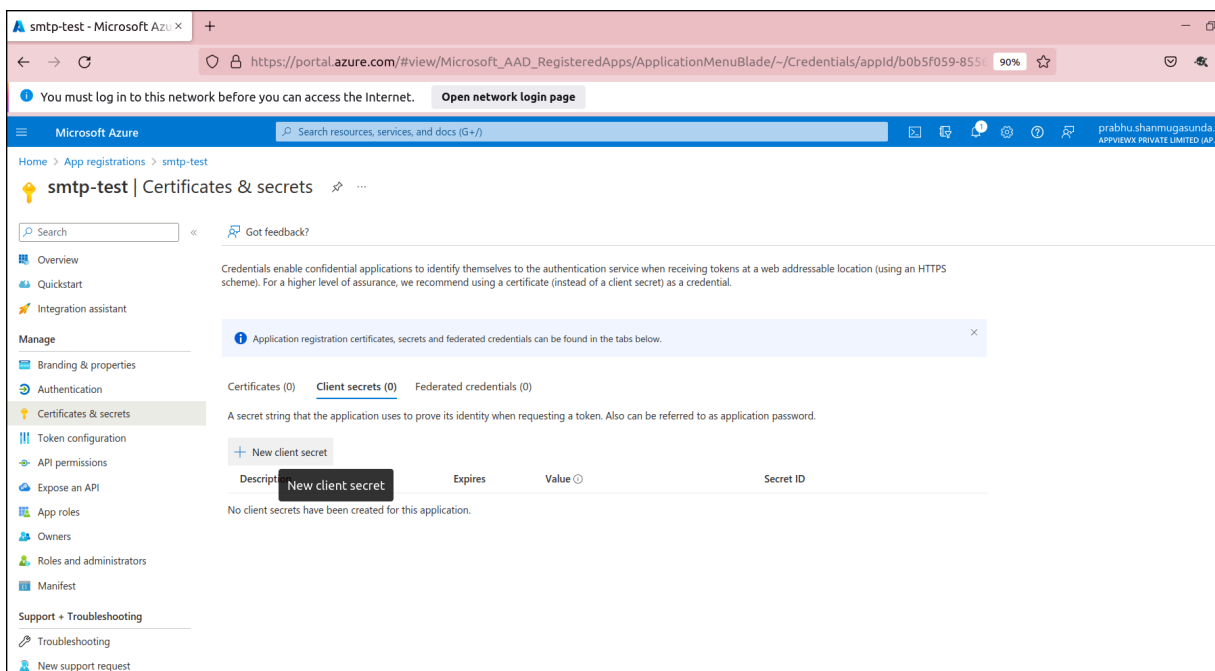


8. Under **Configure platforms**, select **Web** for application type (platform) to configure its settings.

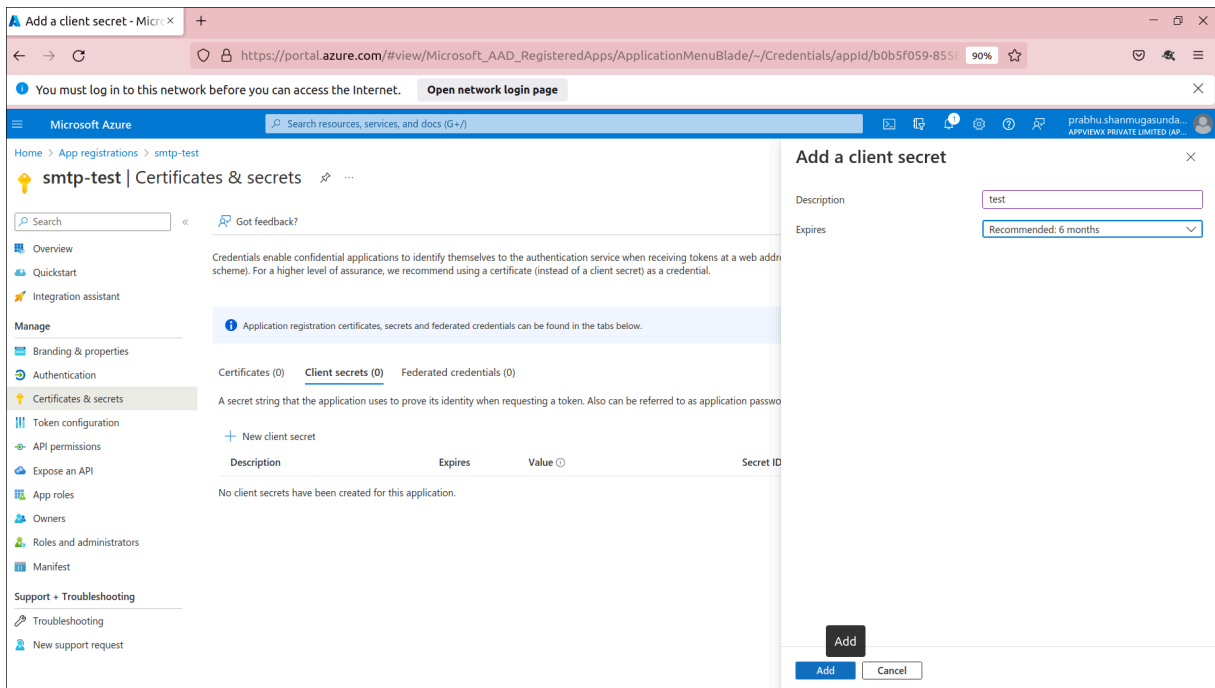
The **Redirect URI :: Configure Web** page is displayed.



9. Enter a **Redirect URI** for your app. This URI is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication.
10. Click **Configure** to complete the platform configuration.
11. Select **Certificates & secrets > Client secrets > New client secret**.

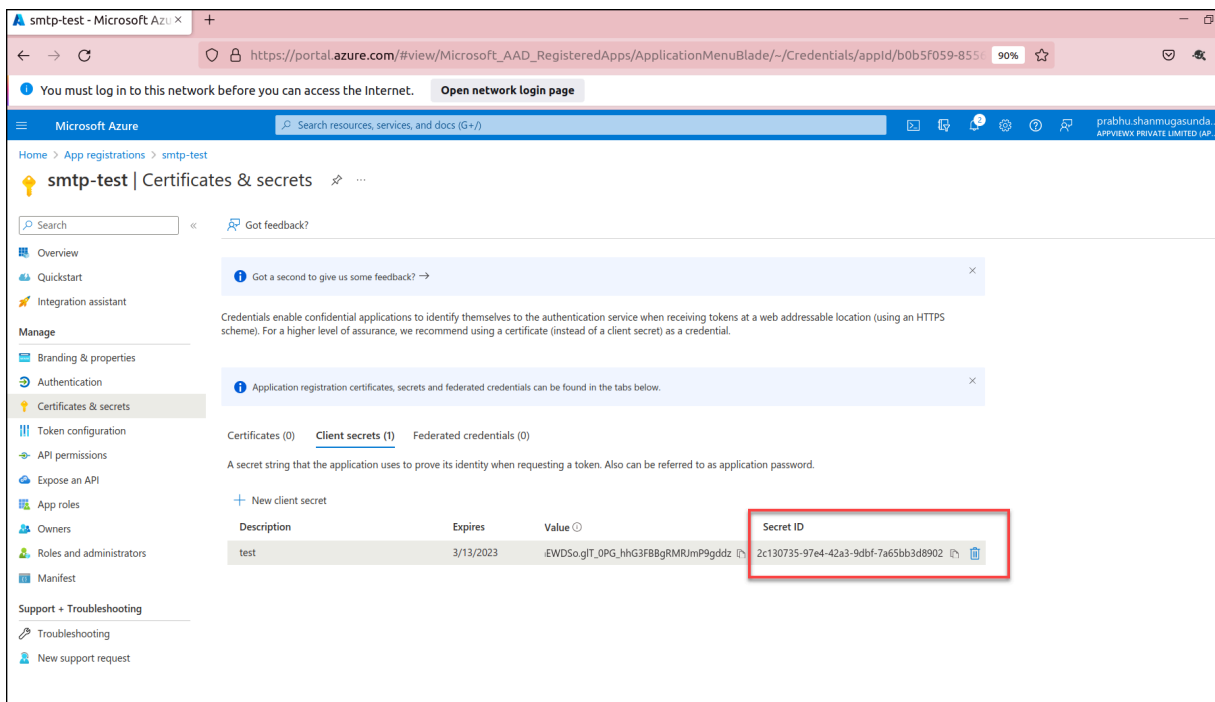


The **New client secret** :: **Add a client secret** page is displayed.



12. Add a **Description** for your client secret.
13. Select an **Expiration** for the secret or specify a custom lifetime.
14. Click **Add**.
15. Record the **Secret value** for use in your client application code.

This secret value is never displayed again after you leave this page.



16. Under **App Registration**, Click **Overview**.

17. Click **Endpoints**.

The **Overview :: Endpoints** page is displayed.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Overview' tab is selected under 'App registrations'. The main content area displays the 'Endpoints' page for the application 'smtp-test'. The 'Endpoints' tab is highlighted in the top navigation bar. The page lists various endpoints for OAuth 2.0 authorization, token, and OpenID Connect. The 'Endpoints' tab is also highlighted in the top navigation bar.

18. Copy **authorization endpoint** and **token endpoint** for Authentication of SMTP Server Settings.

19. Under **Manage**, Click **API permissions**.

The **API permissions** page is displayed.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'API permissions' tab is selected under 'App registrations'. The main content area displays the 'API permissions' page for the application 'smtp-test'. The 'API permissions' tab is highlighted in the top navigation bar. The page shows a table of configured permissions, including 'email', 'offline_access', 'openid', and 'User.Read'. The 'Add a permission' button is highlighted.

API / Permission	Description	Admin consent required	Status
email	Delegated View users' email address	No	...
offline_access	Delegated Maintain access to data you have given it access to	No	...
openid	Delegated Sign users in	No	...
User.Read	Delegated Sign in and read user profile	No	...

20. To add required permissions, Click on **Add a permission**.

The **Request API permissions** page is displayed.

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/all the permissions the application needs. [Learn more about permissions and consent.](#)

+ Add a permission ✓ Grant admin consent for AppViewX Private Limited

API / Permissions name	Type	Description
email	Delegated	View users' email address
offline_access	Delegated	Maintain access to data you have
openid	Delegated	Sign users in
User.Read	Delegated	Sign in and read user profile

To view and manage consented permissions for individual apps, as well as your tenant

21. Click **Microsoft Graph > Delegated permissions**.

Request API permissions

All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

smtp.send

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
SMTP (1)	
SMTP.Send Send emails from mailboxes using SMTP AUTH.	No

Add permissions

Add permissions Discard

22. Under **Select permissions** search box search for the **smtp.send** and select the **SMTP.Send** from the Dropdown.

23. Similarly Search for **email**, **offline_access**, **openid**, **User.Read** and select the **email**, **offline_access**, **openid**, **User.Read** from the respective Dropdowns.

24. Click **Add permissions**.

The **API permissions** added will be Displayed below **API / Permissions name**.

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions), Expose an API, App roles, Owners, Roles and administrators, Manifest, Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled 'smtp-test | API permissions'. It includes a search bar, a refresh button, and a feedback link. A warning message states: 'You are editing permission(s) to your application, users will have to consent even if they've already done so previously.' Below this, an information message explains the 'Admin consent required' column. The 'Configured permissions' section shows a table of permissions for the application 'AppViewX Private Limited'.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				...
email	Delegated	View users' email address	No	...
offline_access	Delegated	Maintain access to data you have given it access to	No	...
openid	Delegated	Sign users in	No	...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	...
User.Read	Delegated	Sign in and read user profile	No	...

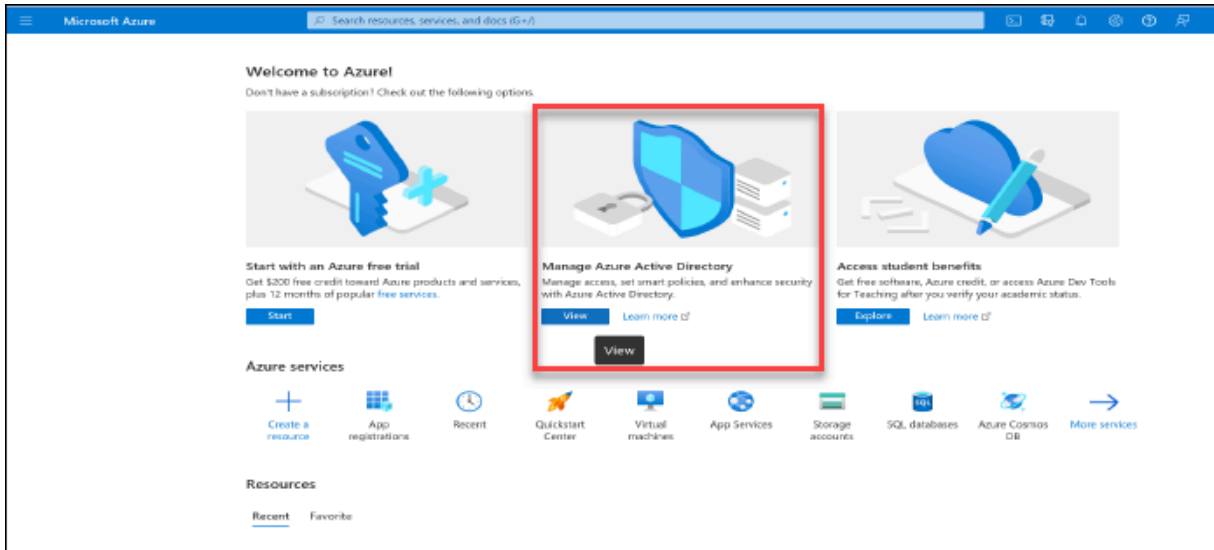
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Frequently Asked Questions

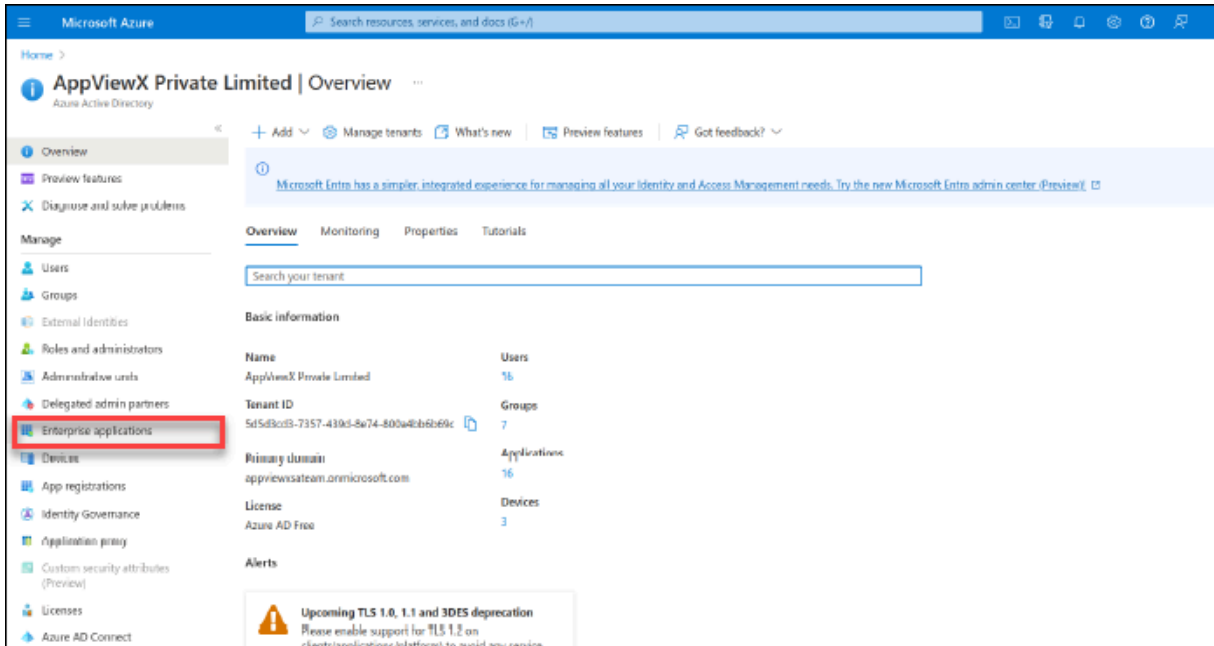
While adding **API permissions** Owner Consent Error is shown, to avoid this error following changes have to be done.

Follow these steps to overcome Owner Consent Error:

1. Microsoft App Registration URL: <https://portal.azure.com/>.
2. Click **Manage Azure Active Directory**.



3. Click on **Enterprise applications** in the left menu.



4. Then click on **Consent and permissions** in the left menu.

Enterprise applications | All applications

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status
SMTP-TEST	0b8373d-2c5a-4d93-92d8-bes5e...	5d11a2d-d515-4512-9e17-b9201...		8/24/2022	-
QANCODE	0b41a6b-d0c9-4e22-9739-9e43a...	6308461e-453a-4956-9382-a3fc52...		9/1/2022	-
AppViewXQANCODE	18150a7f-5158-4f6a-b6da-b35d91...	2c15ad4b-1011-4355-a9cf-dca8251...		9/2/2022	-
QANCODE	313aaa0e-ed47-40c5-b504-98a95...	763fa749-3614-46ba-bb2c-40a0d2...		9/1/2022	-
smtp-test	3337a17-6148-4ec5-b42b-24676...	b0f5059-8556-424c-b96e-2d8b67...		9/13/2022	-
TEST	5689934d-83a4-438b-a116-61a03f...	4a4c1f77-142b-4a4a-9ac7-ef69f4...		9/1/2022	-
Jira Cloud for Excel	635120d-4a20-4f59-9889-c028bb...	d790da92-59d3-4459-b6ee-37648...		1/19/2021	-
SMTP-TEST-GANGA	6c0e55ba-01d4-4b3d-aa04-5723af...	6f0b9eb3-efc5-4543-85bd-923b12...		9/30/2022	-
20.3.0 platformnode	0e42dc07-2deb-4509-06d4-0d423...	3e2c9225-a475-4c12-df14-13065b...		9/27/2022	-
TEST SMTP	97fad500-8f0b-45ca-b257-8f02b1...	7401488a-9caa-4f62-aaaa-1f65252...		9/12/2022	-
newsw	a096ca6f-0262-4174-9a61-172819...	dadb1196-c294-46f9-b41e-b31848...		9/1/2022	-
RC3 build testing	a921e56-2124-4b7f-af93-200e1e2...	53d0efc-7e37-4678-b9ad-fd3964...		9/15/2022	-

5. Change the **User Consent Settings** for User consent for applications from **Do not allow user consent** to **Allow user consent for apps**.
6. Also change the **User Consent Settings** for Group Owner Consent for apps accessing data from **Do not allow group owner consent** to **Allow group owner consent for all group owners**.

Consent and permissions | User consent settings

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

☐ Do not allow user consent
An administrator will be required for all apps.

☐ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

☒ Allow user consent for apps
All users can consent for any app to access the organization's data.

⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. [Learn more about the risks](#)
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". [Learn more](#)

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

☐ Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

☐ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

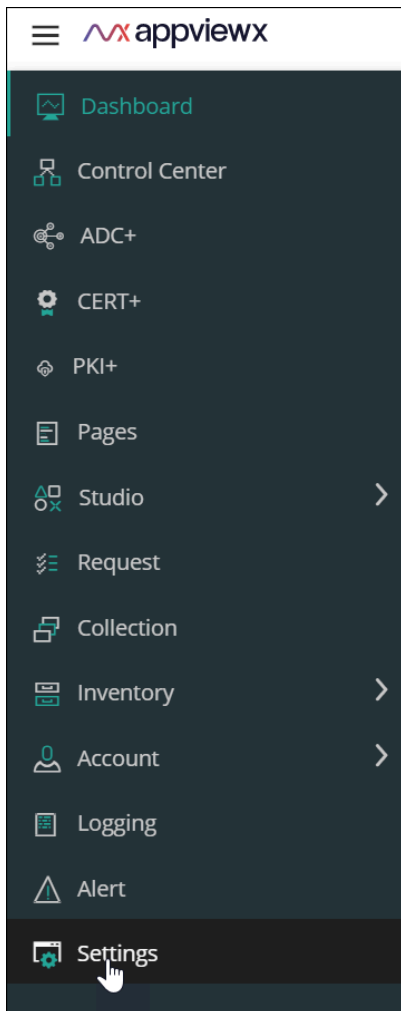
☒ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

Managing Proxy Settings

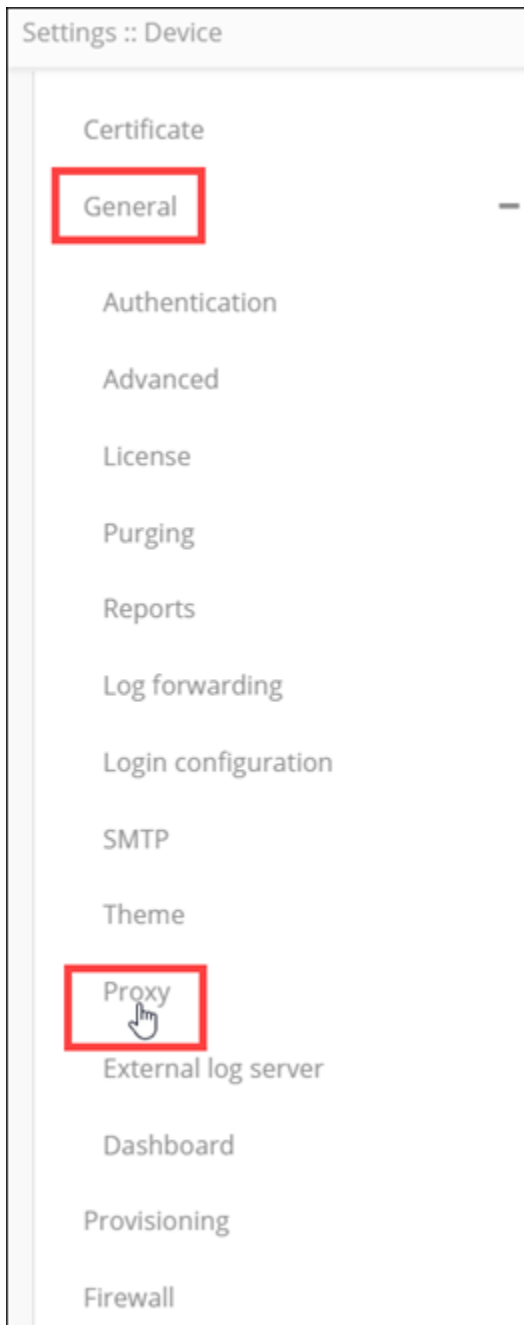
When AppViewX is deployed at a customer's, in order to prevent exposure of the customer's IP address to the internet, AppViewX communicates with the internet using a proxy server.

To configure the proxy settings:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Proxy**.



The **Settings :: Proxy** page is displayed.

5. Enter the following details:

Field	Description
*Proxy Settings	Select the Proxy settings from the following options: • Cloud Connector • AppViewx
*Server name	Name of the proxy server.
*Server IP	IP address of the proxy server.
*Port	Port number of proxy server.
Advanced	To enable advanced settings, select this check box.
Data center	From the drop-down menu, select a data center. Note: This field is displayed only when the Advanced check box is selected.
URL	From the drop-down menu, select the URL. Note: This field is displayed only when the Advanced check box is selected.
Authentication	To enable authentication, select this check box.
*Username	Enter the username.

Field	Description
	 Note: This field is displayed only when the Authentication check box is selected.
*Password	Enter the password.  Note: This field is displayed only when the Authentication check box is selected.
All * marked fields are mandatory.	

6. To save the proxy settings configured above, click **Add**.

The settings are saved and displayed in the table shown in the left half of the screen.

☐	Server name	Conditions	Server IP	Port	Data center	Test connection
☐	SDET_CERT...	URL	192.168.1...	31...	absecon	Test 
Save						

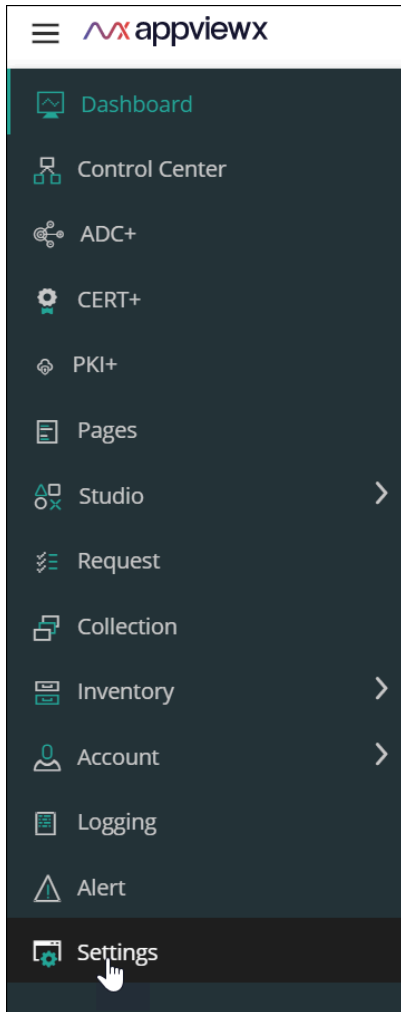
7. To reconfigure the proxy settings, click **Reset**.

Setting the Cryptographic Policy

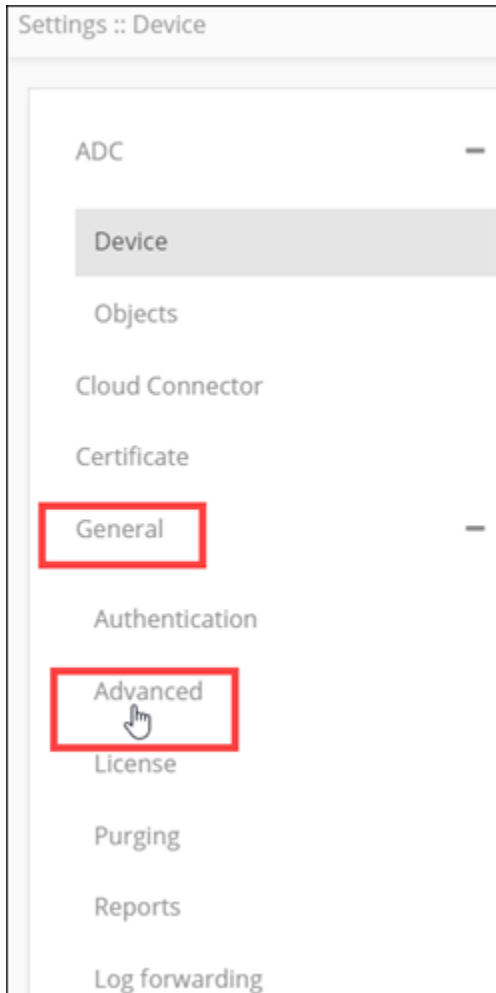
AppViewX enforces a SFTP-based cryptographic policy for protection of sensitive data. Ciphers are used for performing any file operations within AppViewX's functionality and to communicate with devices added in AppViewX.

To set the cryptographic policy:

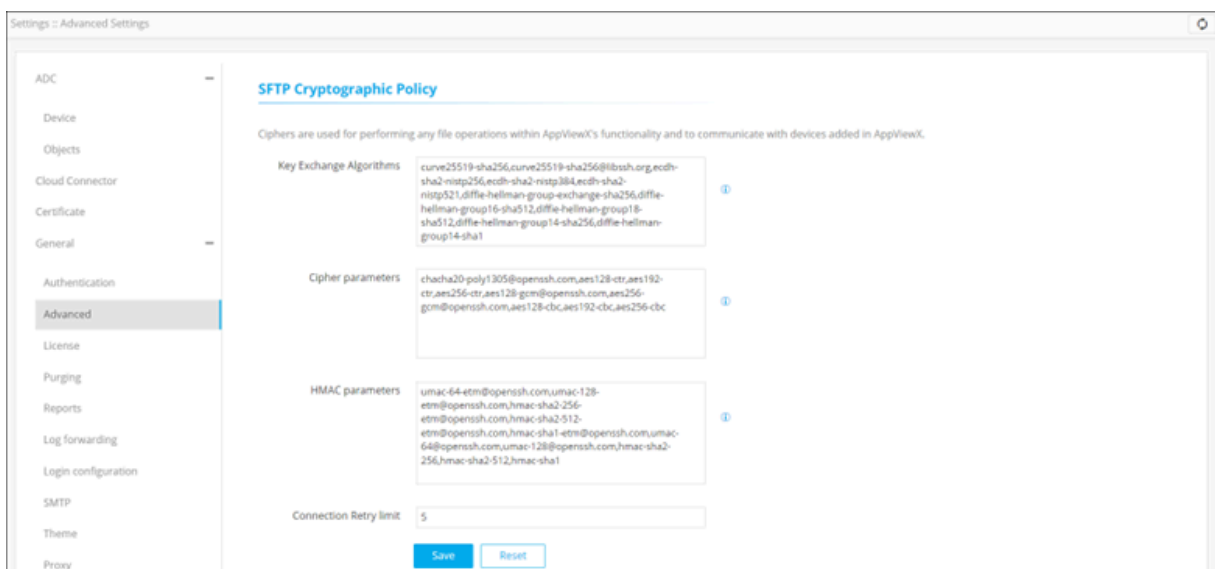
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Advanced**.



The **Settings :: Advanced Settings** page is displayed.



5. In the **SFTP Cryptographic Policy** section, enter the following details:

Field	Description
Key Exchange Algorithms	Algorithms used to exchange keys for a successful handshake between the client and the server.
Cipher parameters	Parameters to encrypt the connection between the client and the server.
HMAC parameters	Parameters to ensure that the received message is intact and not tampered during its delivery from the client to the server and vice versa.
Connection retry limit	Number of attempts to retry establishing a connection between the client and the server.

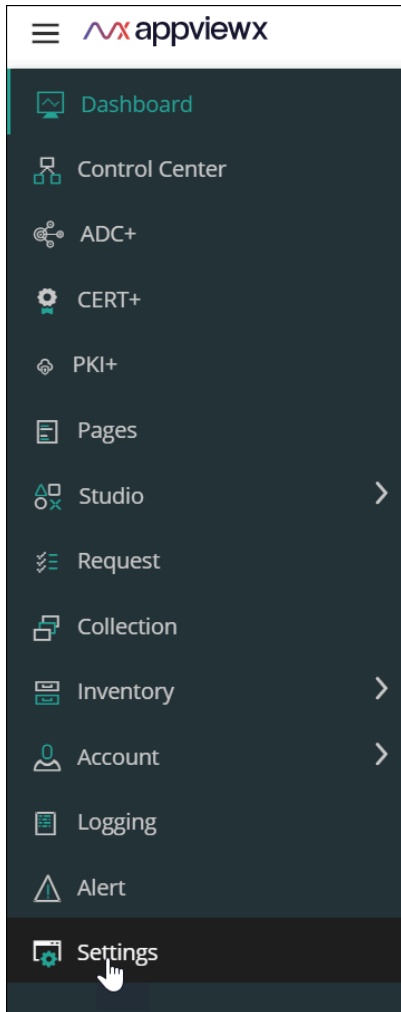
6. Click **Save**.

Enabling Dashboard View for the User

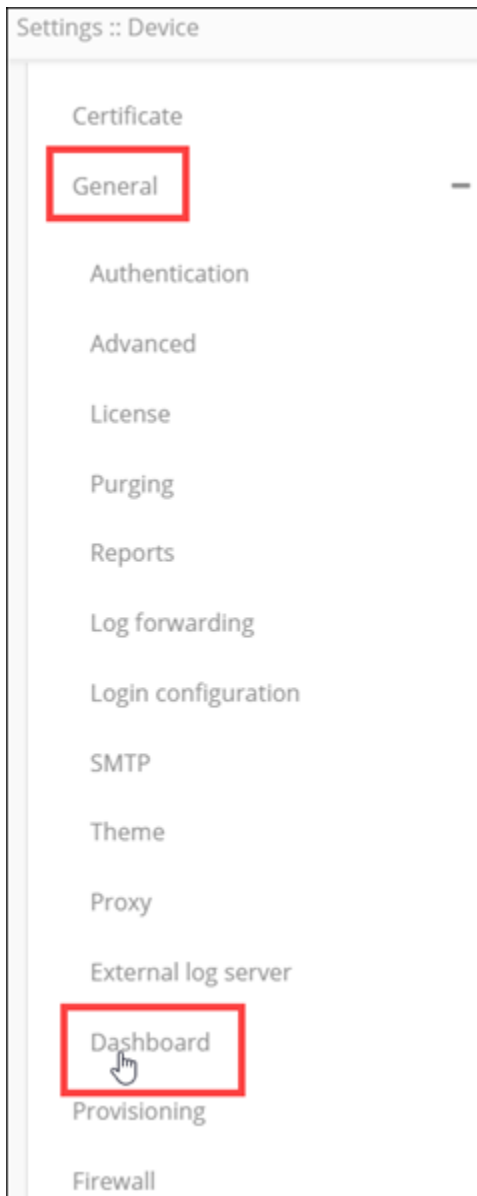
To prevent loss of control over organizational data in the event that a resource leaves the organization, AppViewX lets the admin user have default access to all user dashboard, private as well as public.

To enable default admin access to all dashboards:

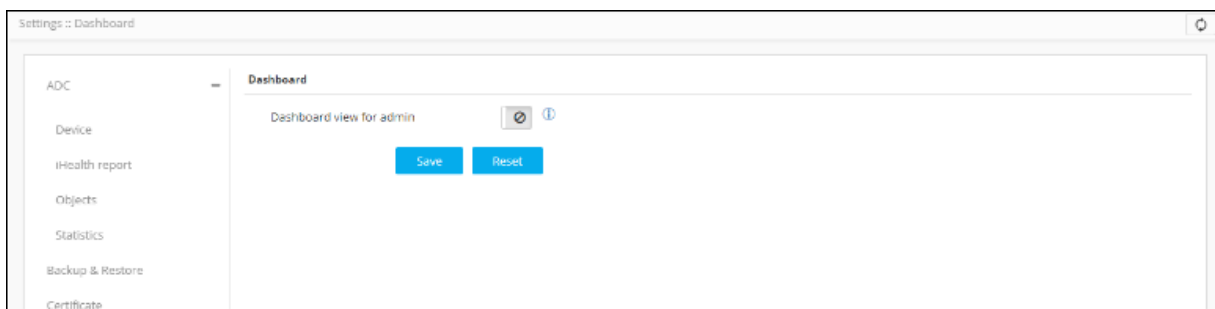
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Dashboard**.



The **Settings :: Dashboard** page is displayed.



5. Turn on the **Dashboard view for admin** toggle and click **Save**.

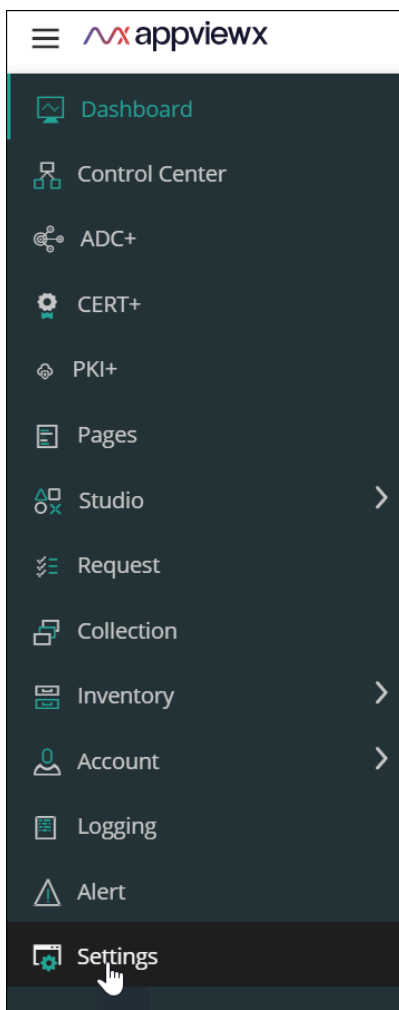
Managing the Login Configuration

- [Restricting the Number of User Sessions](#)
- [Restricting the Number of Login Attempts](#)
- [Managing User Inactivity](#)

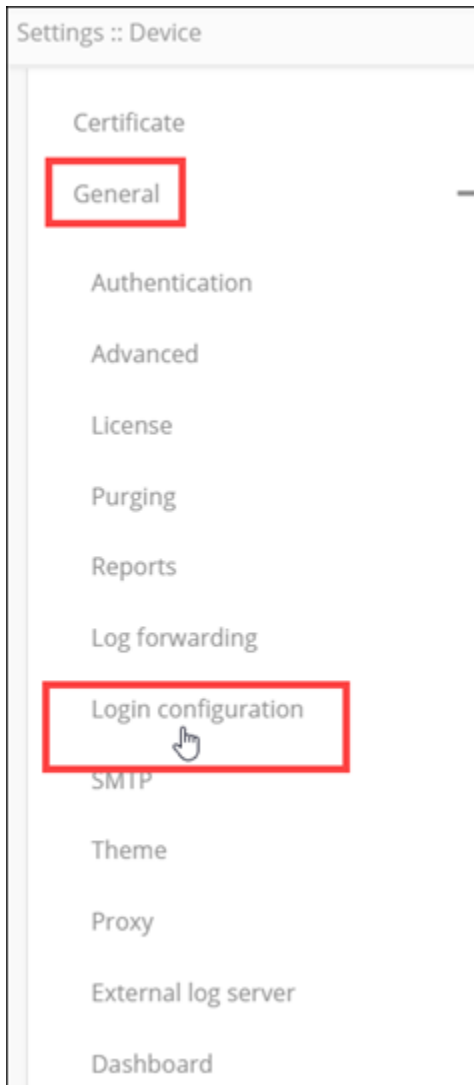
Restricting the Number of User Sessions

The **Restrict each user to a single session** toggle is turned off by default. The number of user sessions can be restricted by enabling this feature.

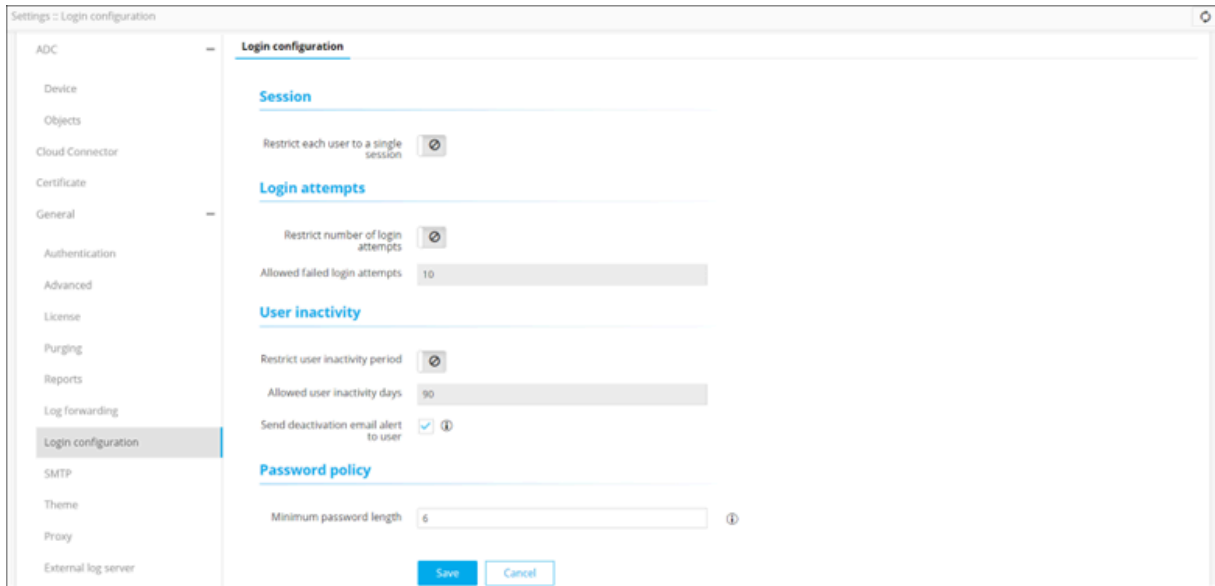
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Login configuration**.



The **Settings :: Login configuration** page is displayed.



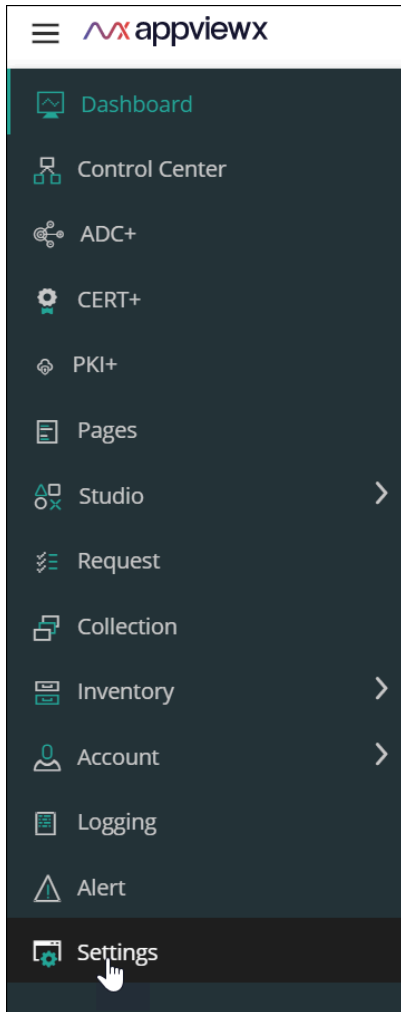
5. In the **Session** section, turn on the **Restrict each user to a single session** toggle.
6. Click **Save**.
7. In the **Confirmation** pop-up, click **OK**.

The Login setting is modified and will be applied from next login for internal users.

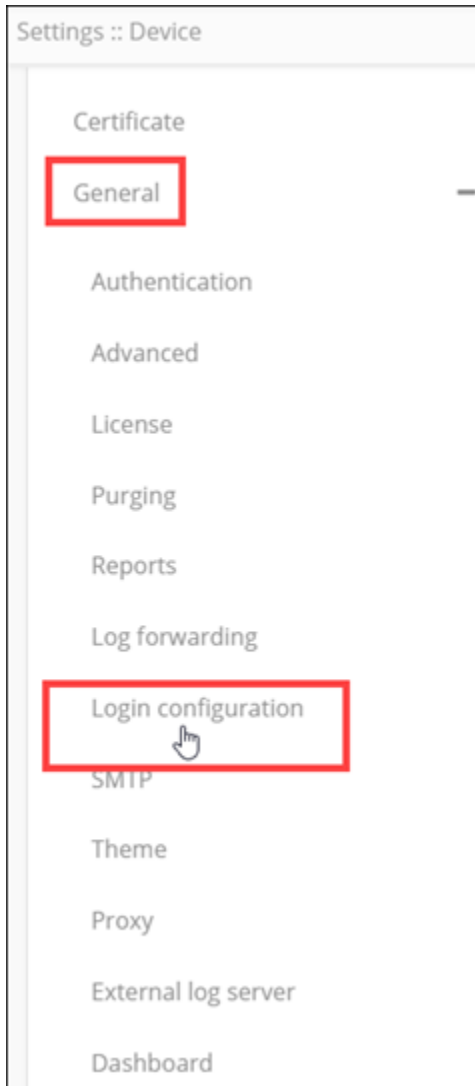
Restricting the Number of Login Attempts

The **Restrict number of login attempts** toggle is turned off by default. The number of login attempts can be restricted by enabling this feature.

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Login configuration**.



The **Settings :: Login configuration** page is displayed.

5. In the **Login attempts** section, enter the following field information:

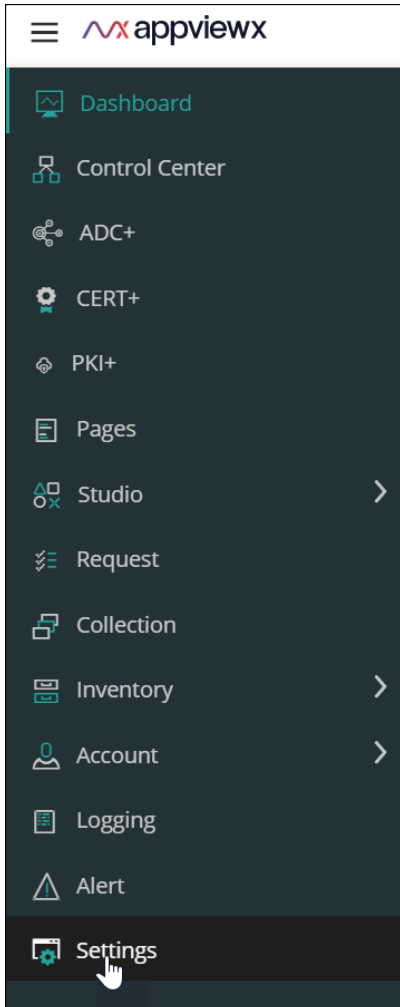
Field	Description
Restrict number of login attempts	Turn on this toggle to restrict the number of login attempts by a user.
Allowed failed login attempts	Enter any number between 0 and 99 to set the number of login attempts permitted.  Note: By default, this value is set to 10. If the user enters incorrect details more than 10 times, he/she will get locked out.

6. Click **Save**.

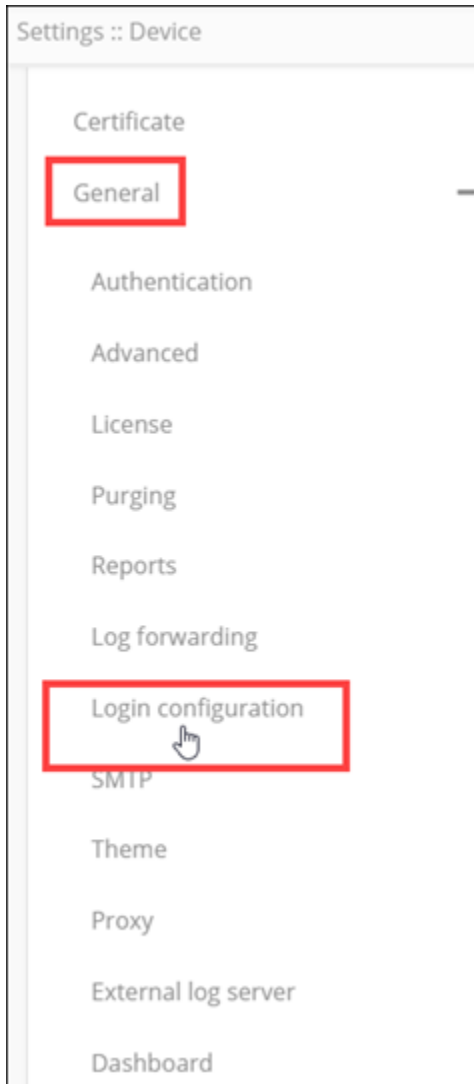
Managing User Inactivity

AppViewX lets you restrict a user from logging in to the system if they have been inactive for a predefined duration.

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Login configuration**.



The **Settings :: Login configuration** page is displayed.

Settings :: Login configuration

ADC

Device

Objects

Cloud Connector

Certificate

General

Authentication

Advanced

License

Purging

Reports

Log forwarding

Login configuration

SMTP

Theme

Proxy

External log server

Login configuration

Session

Restrict each user to a single session ☐

Login attempts

Restrict number of login attempts ☐

Allowed failed login attempts 10

User inactivity

Restrict user inactivity period ☐

Allowed user inactivity days 90

Send deactivation email alert to user ☒

Password policy

Minimum password length 6

Save Cancel

5. In the **User inactivity** section, turn on the **Restrict user inactivity period** toggle.
6. To set the number of days for which a user can remain inactive, in the **Allowed user inactivity days** text field, enter the required value (between 0 and 99).
7. To send the user an email when they are deactivated, select the **Send deactivation email alert to user** check box.
An email alert is sent to the user for three consecutive days before deactivation.
8. Click **Save**.

Chapter 6: Managing Logs

- [Overview](#)
- [Viewing Logs](#)
- [Setting the Record Count Preference for Logs](#)
- [Searching for Logs](#)
- [Forwarding Logs](#)
- [Exporting Logs](#)
- [Purging Logs](#)

Overview

Log management is an integral part of any customer-serving application. Monitoring and analyzing user activity logs helps in preventing security breaches, provides an insight into the performance of the applications, and contributes to troubleshooting.

As a part of log management, AppViewX tracks user activities and creates device and object level logs. For all recorded logs, it lets you:

- View logs
- Filter logs
- Forward logs
- Export logs
- Purge logs

AppViewX lets you view all logs in one place as well as groups them under the following types for a segregated viewing:

- All
- Audit
- Self Audit
- Certificate
- ADC
- AppViewX
- Syslog
- SSH

Viewing Logs

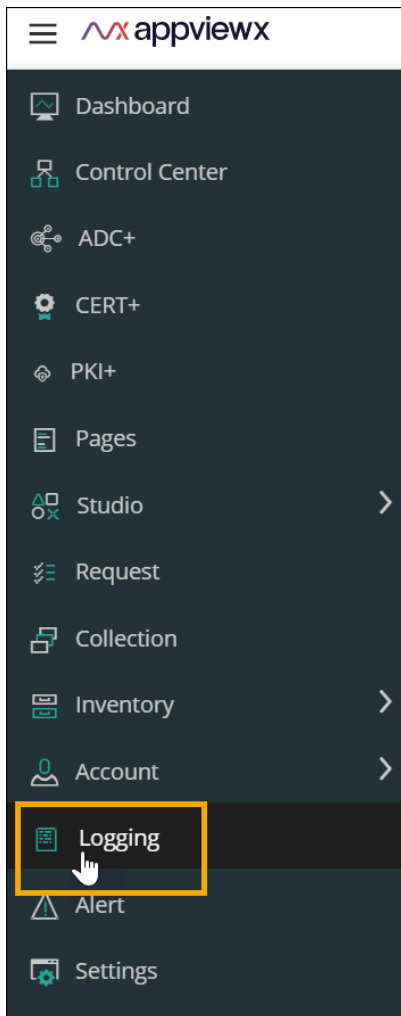
AppViewX supports only role-based (and not user-based) access for logs, which means that if a user role has permission to view logs, all users under that user role can view all AppViewX logs.

- [Viewing All Logs](#)
- [Viewing ADC Logs](#)
- [Viewing AppViewX Logs](#)
- [Viewing Audit Logs](#)
- [Viewing Certificate Logs](#)
- [Viewing Self-Audit Logs](#)
- [Viewing SSH Logs](#)
- [Viewing Syslog Logs](#)
- [Viewing Workflow Logs](#)

Viewing All Logs

To view all logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

Logging :: All 1 to 25 of 17,692

All Audit Self Audit Workflow Certificate ADC AppViewX Firewall						
Q Search...						
Time	User	Device name	Object details	Log category	Severity	Log message
07/28/2022 11:20:07 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 11:16:01 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 11:10:14 AM	system			Audit	Notification	Workflow Temporary request : temp_138 is deleted from Database succes...
07/28/2022 11:10:13 AM	system			VisualWorkflow	Notification	Stop Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/28/2022 11:10:12 AM	system			VisualWorkflow	Notification	Script Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/28/2022 11:10:12 AM	system			VisualWorkflow	Notification	Initiating Script[Transaction Id : cron-1852279cb3-local-1824351b459]
07/28/2022 11:10:12 AM	system			VisualWorkflow	Notification	[{"response":null,"message":null,"appStatusCode":null,"tags":null,"headers...
07/28/2022 11:10:11 AM	system			VisualWorkflow	Notification	[{"subsystemDetails":{"subsystem":"adc","licenseInfo":{"name":"objectCou...
07/28/2022 11:10:11 AM	system			VisualWorkflow	Notification	Script Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/28/2022 11:10:11 AM	system			VisualWorkflow	Notification	[{"default":{"objectCount":0,"certificateCount":3,"deviceCount":0}][Transac...
07/28/2022 11:10:11 AM	system			VisualWorkflow	Notification	Initiating Script[Transaction Id : cron-1852279cb3-local-1824351b459]
07/28/2022 11:10:07 AM	system			VisualWorkflow	Notification	Script Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/28/2022 11:10:06 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 11:06:01 AM	System			AppViewX	Critical	License Details Completed[Transaction Id : cron-1852279cb3-local-182435...
07/28/2022 11:06:01 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 11:00:08 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:56:02 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:50:06 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:46:01 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:40:06 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:36:02 AM	admin			Audit	Notification	User: admin in User Group: [admin usergroup] logged in as an internal user
07/28/2022 10:36:02 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:30:08 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...
07/28/2022 10:26:02 AM	System			AppViewX	Critical	All Cloud Connectors are down. No Cloud Connector available to serve re...

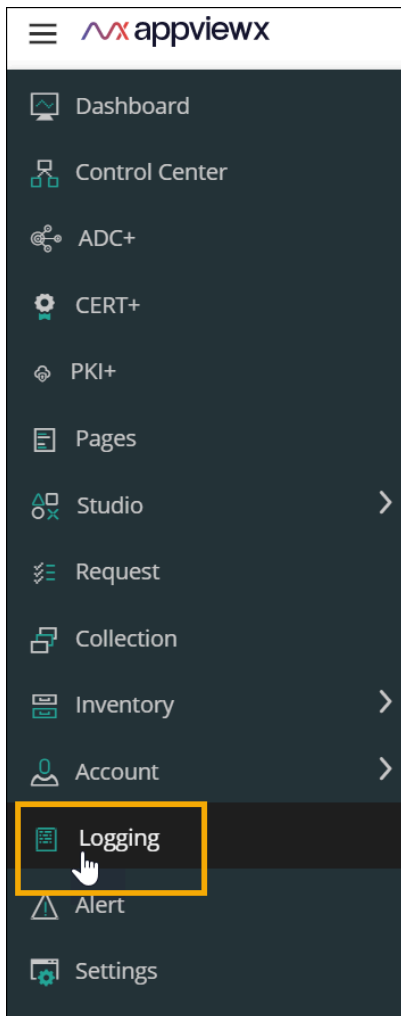
For each activity, this page displays the following details:

Category	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Log category	Category under which this log record will be filed
Severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing ADC Logs

To view the ADC logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **ADC** tab.

The **Logging :: ADC** page is displayed.

Time	User	Device name	Object details	Alert severity	Log message
03/16/2021 05:30:25 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/16/2021 05:30:22 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/15/2021 12:44:06 PM	admin	12.34.5.4		Critical	Config fetch action failed for device 1...
03/15/2021 12:44:04 PM	admin	12.34.5.4		Notification	Config fetch action triggered on the d...
03/15/2021 05:30:26 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/15/2021 05:30:19 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/14/2021 05:30:27 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/14/2021 05:30:22 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/13/2021 05:30:28 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/13/2021 05:30:06 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/12/2021 05:30:28 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/12/2021 05:30:25 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/11/2021 05:30:29 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/11/2021 05:30:22 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/10/2021 05:30:27 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/10/2021 05:30:19 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/09/2021 05:30:29 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...
03/09/2021 05:30:26 AM	system	12.34.5.4		Notification	Config fetch action triggered on the d...
03/07/2021 05:30:18 AM	system	12.34.5.4		Critical	Config fetch action failed for device 1...

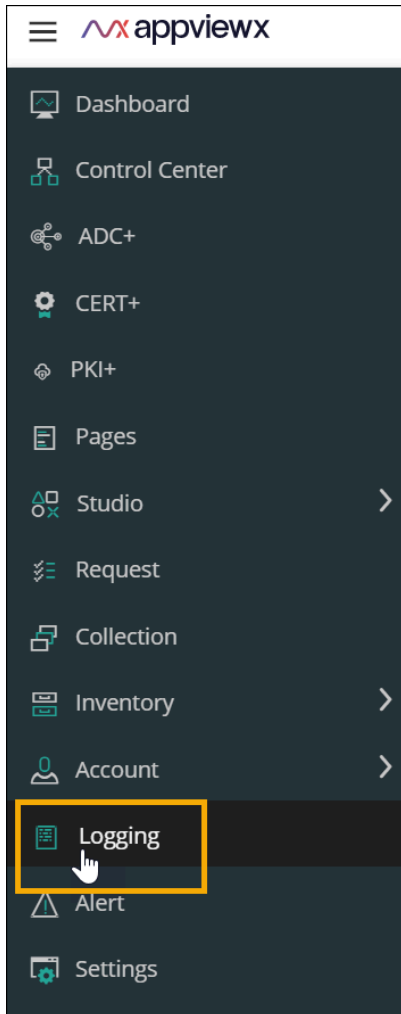
The page displays the following details for the ADC logs:

Category	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Alert severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing AppViewX Logs

To view the AppViewX logs:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **AppViewX** tab.

The **Logging :: AppViewX** page is displayed.

Logging : AppViewX 1 to 25 of 16,354

All Audit Self Audit Workflow Certificate ADC **AppViewX** Firewall

Q Search... Log message

Time	Device name	Object details	Severity	Log message
07/28/2022 11:36:03 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:30:08 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:26:02 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:20:07 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:16:01 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:10:06 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:06:01 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 11:00:08 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:56:02 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:50:06 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:46:01 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:40:06 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:36:02 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:30:08 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:26:02 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:20:07 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:16:02 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:10:05 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:06:02 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 10:00:07 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 09:56:01 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 09:50:07 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 09:46:01 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 09:40:06 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...
07/28/2022 09:36:01 AM			▲ Critical	All Cloud Connectors are down. No Cloud Connector available to serve requests.[Transaction Id : cron...

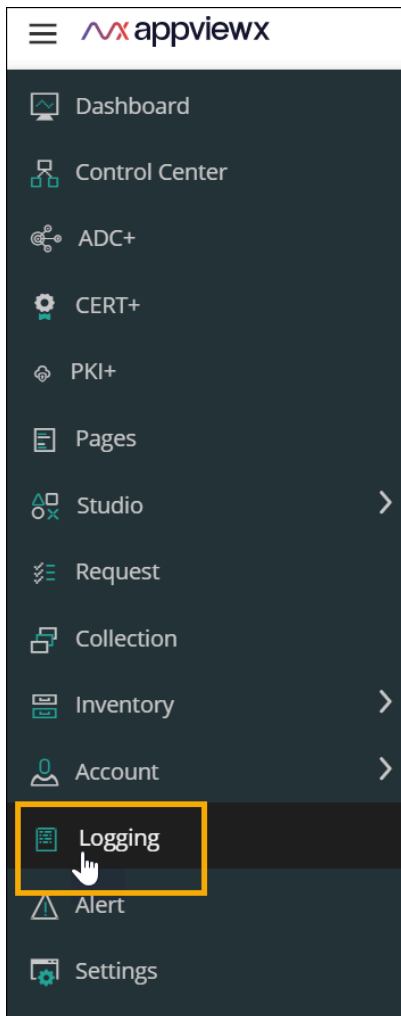
The page displays the following details for the AppViewX logs:

Category	Description
Time	Date and time at which the activity was carried out
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing Audit Logs

To view Audit logs,

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Audit** tab.

The **Logging :: Audit** page is displayed.

Logging : Audit

1 to 25 of 359

All **Audit** Self Audit Workflow Certificate ADC AppViewX Firewall

Q Search...

Time	User	Device name	Object details	Source IP	AppViewX n...	Method of l...	Comments	Log message
07/28/2022 11:10:14 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_138 is deleted from ...
07/28/2022 10:38:08 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/28/2022 09:41:26 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/28/2022 08:50:53 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/27/2022 01:43:17 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/27/2022 11:10:15 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_137 is deleted from ...
07/26/2022 04:41:31 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 03:30:35 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 03:00:14 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 03:00:00 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/26/2022 02:59:59 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/26/2022 11:10:14 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_136 is deleted from ...
07/25/2022 04:51:08 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/25/2022 02:31:28 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/25/2022 11:10:15 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_135 is deleted from ...
07/25/2022 10:32:13 ...	admin		NA	192.168.124...	avx-common...	UI		All log file exported successfully(Transaction Id : WEB-Snfc...
07/25/2022 10:31:27 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/25/2022 10:31:14 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/25/2022 10:31:14 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/24/2022 11:10:14 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_134 is deleted from ...
07/23/2022 11:10:15 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_133 is deleted from ...
07/22/2022 11:10:13 ...	system			127.0.0.1	172.30.2.19	AppViewX		Workflow Temporary request : temp_132 is deleted from ...
07/22/2022 10:28:12 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/21/2022 02:21:46 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/21/2022 01:33:18 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...

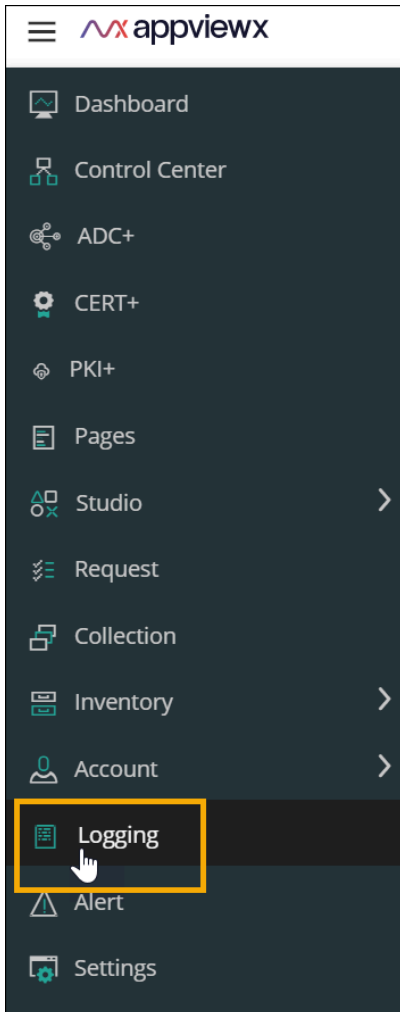
The page displays the following details for the Audit logs:

Category	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Source IP	IP address of the system that was the source of the activity.
AppViewX node	IP address of the installed AppViewX node.
Method of login	The method used for logging in to the AppViewX node, from one of the following: • UI • AppViewX (used for cronjob-related activities)
Comments	Comments related to the activity logged.
Log Message	Description of the activity logged

Viewing Certificate Logs

To view Certificate logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Certificate** tab.

The **Logging :: Certificate** page is displayed.

Logging :: Certificate

1 to 25 of 31

All Audit Self Audit Workflow **Certificate** ADC AppViewX Firewall

Q Search...

Log Message

Time	User	Device Name	Object Details	Purpose/Usage	Severity	Log Message
06/01/2022 11:39:25 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:39:20 AM	admin	NA	test1	Server	Debug	Request by admin to Revoke the certificate with common name test1 is suc...
06/01/2022 11:39:20 AM	admin	NA	test1	Server	Notification	Revoke Completion :: The certificate requested by user : admin belonging t...
06/01/2022 11:39:20 AM	admin	NA	test1	Server	Debug	admin has requested to Revoke the certificate with common name test1. T...
06/01/2022 11:39:20 AM	admin	NA	test1	Server	Notification	Revoke Initiation :: User : admin belonging to user group(s) : [admin usergr...
06/01/2022 11:39:15 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:39:05 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:45 AM	admin	NA	test1	Server	Debug	Request by admin to Submit the certificate with common name test1 is suc...
06/01/2022 11:38:45 AM	admin	NA	test1	Server	Notification	Create/Regenerate Completion :: The certificate requested by user : admin ...
06/01/2022 11:38:45 AM	admin	NA	test1	Server	Notification	Create/Regenerate Completion :: The certificate requested by user : admin ...
06/01/2022 11:38:45 AM	admin	NA	test1	Server	Debug	admin has requested to Submit the certificate with common name test1. Th...
06/01/2022 11:38:45 AM	admin	NA	test1	Server	Notification	Create/Regenerate Initiation :: User : admin belonging to user group(s) : [ad...
06/01/2022 11:38:45 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:39 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:35 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:25 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:25 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:02 AM	admin	NA	test1	Server	Notification	Holistic view: Server certificate with Common name: test1 and Serial numb...
06/01/2022 11:38:00 AM	admin	NA	test1	Server	Notification	CA Connector modification: AppViewX CA connector has been updated suc...
05/20/2022 04:18:44 PM	admin	NA	ip-172-30-2-19.ap-so...	Server	Notification	Holistic view: Server certificate with Common name: ip-172-30-2-19.ap-sout...
05/02/2022 03:00:55 PM	admin	pe-pltf-node16.lab.a...	NA	NA	Debug	Request by admin to fetch configuration of the device pe-pltf-node16.lab.a...
05/02/2022 03:00:54 PM	admin	pe-pltf-node16.lab.a...	NA	NA	Debug	admin has requested to fetch configuration of the device pe-pltf-node16.la...
05/02/2022 02:58:40 PM	admin	NA	NA	Server	Debug	Certificate has been downloaded by the user: admin. The response compris...
05/02/2022 02:58:38 PM	admin	NA	pe-pltf-node16.lab.a...	Server	Notification	Certificate download:Server certificate with Common name: pe-pltf-node16...

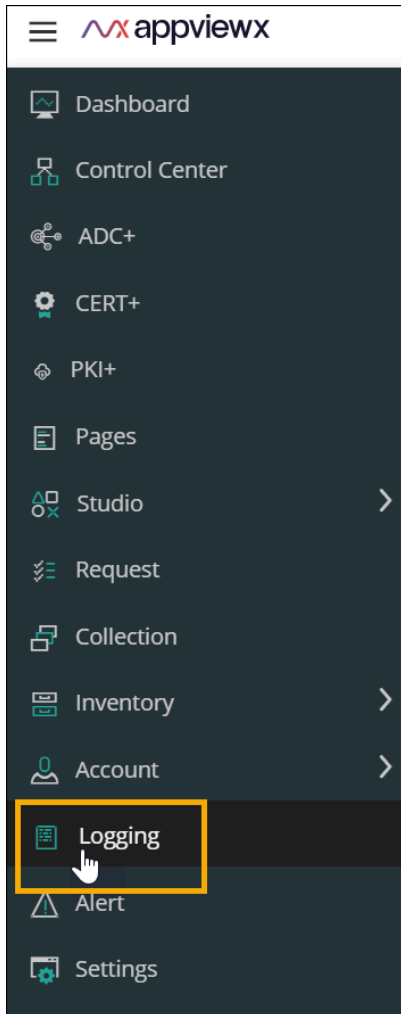
The page displays the following details for the Certificate logs:

Category	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity.
Object details	Name of the object, if the log is of a object-related activity.
Purpose/Usage	Certificate type (server, client, device, code signing) associated with the logged activity.
severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical).
Log Message	Description of the activity logged.

Viewing Self-Audit Logs

To view Self Audit logs:

- To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
- From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Self Audit** tab.

The **Logging :: Self Audit** page is displayed.

Logging :: Self Audit 1 to 25 of 177

[All](#)
[Audit](#)
[Self Audit](#)
[Workflow](#)
[Certificate](#)
[ADC](#)
[AppViewX](#)
[Firewall](#)

Q Search... Log message

Time	User	Device name	Object details	Source IP	AppViewX n...	Method of L...	Comments	Log message
07/26/2022 10:38:08 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 09:41:26 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 08:50:53 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/27/2022 01:43:17 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 04:41:31 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 03:30:35 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 03:00:14 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/26/2022 03:00:00 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/26/2022 02:59:59 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/25/2022 04:51:08 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/25/2022 02:31:28 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/25/2022 10:32:13 ...	admin		NA	192.168.124...	avx-common...			All log file exported successfully(Transaction id : WEB-Sof...
07/25/2022 10:31:27 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/25/2022 10:31:14 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/25/2022 10:31:14 ...	admin			192.168.124...		UI		Login failed for user: admin due to incorrect credentials
07/22/2022 10:28:12 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/21/2022 02:21:46 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/21/2022 01:33:18 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/19/2022 12:32:11 ...	admin			192.168.236...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/18/2022 05:27:09 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/18/2022 05:03:54 ...	admin			192.168.124...	avx-platform...	UI		Role: xxxx has been created by user: admin(Transaction L...
07/18/2022 04:54:23 ...	admin			192.168.124...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/13/2022 02:32:58 ...	admin			192.168.236...		UI		User: admin in User Group: [admin usergroup] logged in a...
07/13/2022 02:32:43 ...	admin			192.168.236...		UI		User: admin in User Group: [admin usergroup] logged out...
07/13/2022 02:32:16 ...	admin			192.168.236...		UI		User: admin in User Group: [admin usergroup] logged in a...

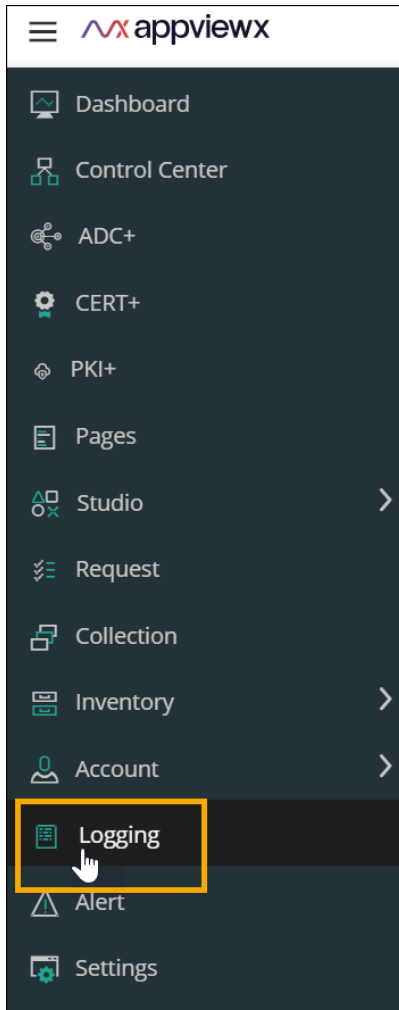
The page displays the following details for the Self Audit logs:

Category	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Source IP	IP address of the system that was the source of the activity.
AppViewX node	IP address of the installed AppViewX node.
Method of login	The method used for logging in to the AppViewX node, from one of the following: • UI • AppViewX (used for cronjob-related activities)
Comments	Comments related to the activity logged.
Log Message	Description of the activity logged

Viewing SSH Logs

To view the SSH logs:

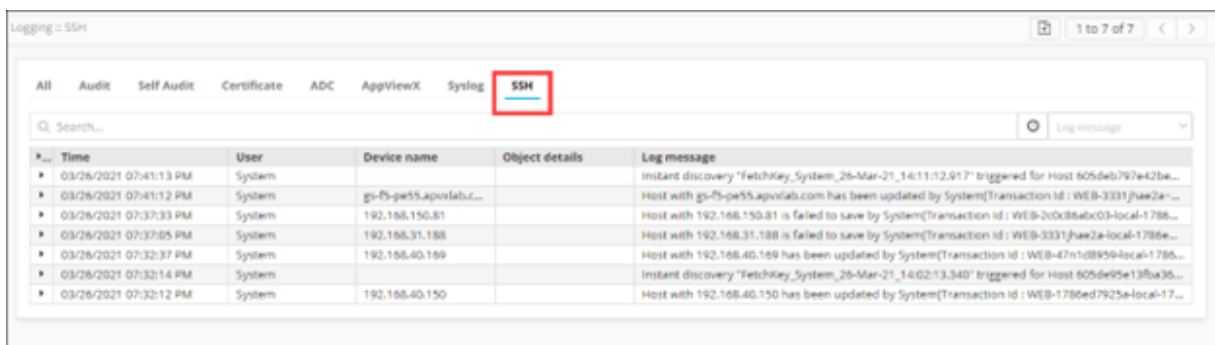
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **SSH** tab.

The **Logging :: SSH** page is displayed.



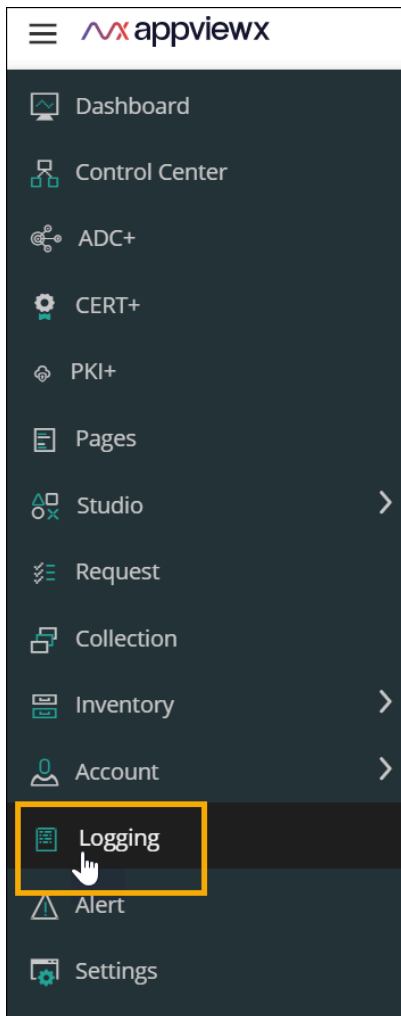
The page displays the following details for the SSH logs:

Category	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Log Message	Description of the activity logged

Viewing Syslog Logs

To view the Syslog logs:

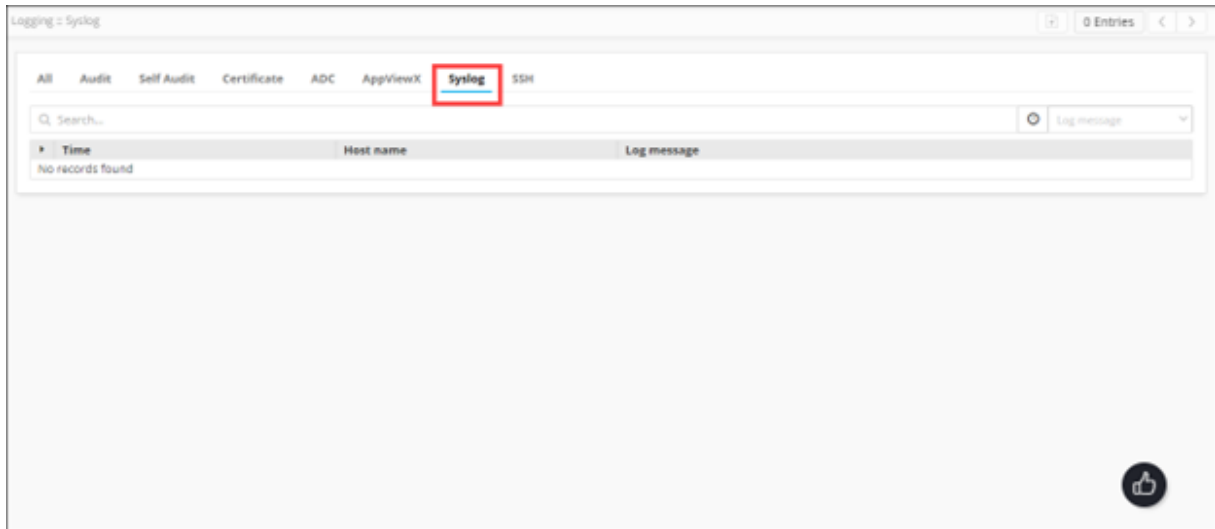
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Syslog** tab.

The **Logging :: Syslog** page is displayed.



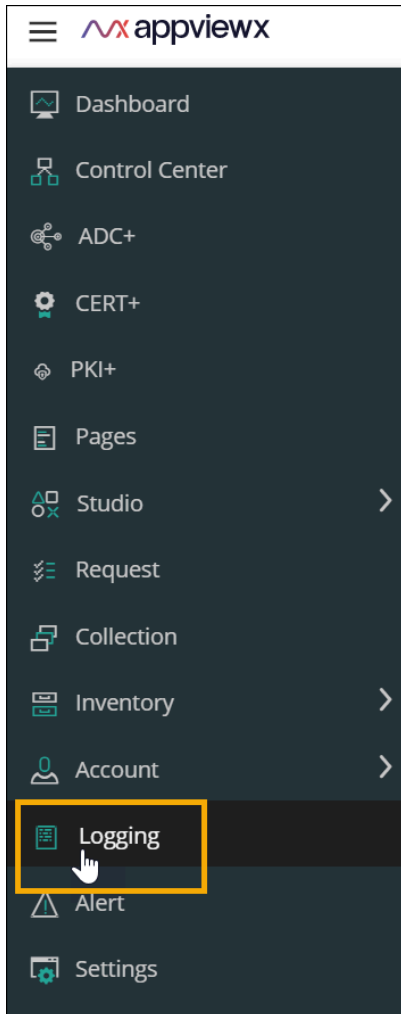
The page displays the following details for the Syslog logs:

Category	Description
Time	Date and time at which the activity was carried out.
Host name	Host name of the Syslog server.
Log Message	Description of the activity logged.

Viewing Workflow Logs

To view the workflow logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Workflow** tab.

The **Logging :: Workflow** page is displayed.

Logging :: Workflow 1 to 25 of 951

All Audit Self Audit **Workflow** Certificate ADC AppViewX Firewall

Q Search... Log message

Time	Request ID	User	Work order stage	Workflow	Alert severity	Log message
07/26/2022 11:10:13 AM	temp_138	system	workflow_stop_1	License_check	Notification	Stop Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:12 AM	temp_138	system	script_3	License_check	Notification	Script Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:12 AM	temp_138	system	script_3	License_check	Notification	Initiating Script[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:12 AM	temp_138	system	script_3	License_check	Notification	[{"response":null,"message":null,"appStatusCode":null,"tags":null,"headers":null...]
07/26/2022 11:10:11 AM	temp_138	system	script_1	License_check	Notification	[{"subsystemDetails":{"subsystem":"adc","licenseInfo":{"name":"objectCou...}}
07/26/2022 11:10:11 AM	temp_138	system	script_1	License_check	Notification	Script Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:11 AM	temp_138	system	script_1	License_check	Notification	[{"default":{"objectCount":0,"certificateCount":3,"deviceCount":0}}][Transact...
07/26/2022 11:10:11 AM	temp_138	system	script_1	License_check	Notification	Initiating Script[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:07 AM	temp_138	system	script_2	License_check	Notification	Script Completed[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:07 AM	temp_138	system	script_2	License_check	Notification	Initiating Script[Transaction Id : cron-1852279cb3-local-1824351b459]
07/26/2022 11:10:05 AM	temp_138	system	createform_2	License_check	Notification	License Details Completed[Transaction Id : cron-1852279cb3-local-1824351b4...
07/27/2022 11:10:15 AM	temp_137	system	workflow_stop_1	License_check	Notification	Stop Completed[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:14 AM	temp_137	system	script_3	License_check	Notification	Script Completed[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:14 AM	temp_137	system	script_3	License_check	Notification	[{"response":null,"message":null,"appStatusCode":null,"tags":null,"headers":null...]
07/27/2022 11:10:14 AM	temp_137	system	script_3	License_check	Notification	Initiating Script[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:12 AM	temp_137	system	script_1	License_check	Notification	Script Completed[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:12 AM	temp_137	system	script_1	License_check	Notification	[{"subsystemDetails":{"subsystem":"adc","licenseInfo":{"name":"objectCou...}}
07/27/2022 11:10:12 AM	temp_137	system	script_1	License_check	Notification	[{"default":{"objectCount":0,"certificateCount":3,"deviceCount":0}}][Transact...
07/27/2022 11:10:10 AM	temp_137	system	script_1	License_check	Notification	Initiating Script[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:10 AM	temp_137	system	script_2	License_check	Notification	Script Completed[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:10 AM	temp_137	system	script_2	License_check	Notification	Initiating Script[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/27/2022 11:10:06 AM	temp_137	system	createform_2	License_check	Notification	License Details Completed[Transaction Id : cron-52c65c9fe-local-1823e2b5810]
07/26/2022 11:10:13 AM	temp_136	system	workflow_stop_1	License_check	Notification	Stop Completed[Transaction Id : cron-5a4038577c6-local-1823904f93d]
07/26/2022 11:10:12 AM	temp_136	system	script_3	License_check	Notification	Script Completed[Transaction Id : cron-5a4038577c6-local-1823904f93d]
07/26/2022 11:10:12 AM	temp_136	system	script_3	License_check	Notification	[{"response":null,"message":null,"appStatusCode":null,"tags":null,"headers":null...]

The page displays the following details for the Workflow logs:

Category	Description
Time	Date and time at which the activity was carried out.
Request ID	Workflow Request ID
User	Username of the user who performed the activity.
Work order stage	The stage at which an action is performed on the workflow.
Alert severity	Severity of the workflow.
Log Message	Description of the activity logged.

Setting the Record Count Preference for Logs

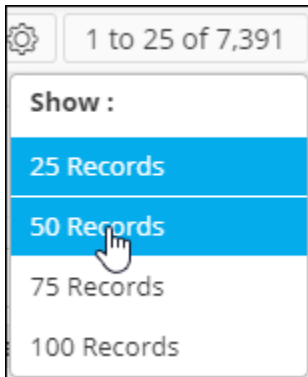
For easier viewing of records, AppViewX lets you set the record count preference, which is the number of log records that will be displayed on one page.



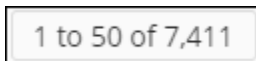
Note: By default, 100 records are shown on one page (which is why the control reads 1 to 100).

To set the record count preference:

1. On the **Logging :: All** page, from the top-right corner of the screen, click  .
2. From the **Show** menu displayed, select your record count preference (for example, 25 records).



3. The Logging page is updated according to the record count preference selected. A message, **Record count preference saved successfully**, is displayed. The UI control is also updated to display the current selection, as shown in the following image:



Searching for Logs

AppViewX lets you search for logs in two ways:

- Based on a timestamp
- Based on the values recorded for each log
- [Based on a Timestamp](#)
- [Based on the Values Recorded for each Log](#)

Based on a Timestamp

To search for logs based on a timestamp:

1. From the **Search** field on the **Logging** page, click  .
2. Widgets to select the date and time are displayed.

The screenshot shows a web interface for selecting a date range and time. It consists of two main sections, 'From:' and 'To:', each containing a calendar and a time picker. Both calendars are for March 2021, with the 16th selected. The time pickers are set to 12:00:00 AM. At the bottom right, there are 'Reset' and 'OK' buttons.

3. To select a date range, in the **From** and **To** fields, select the required dates.
4. To set a time, use the **Hour**, **Minute**, and **Second** slider controls.
5. Click **OK**.

The page is updated to display log records from the selected timestamp.



Note: To view records from a specific date to the current date, select only the From date. When the To field is left blank, by default, it is set to the current date.

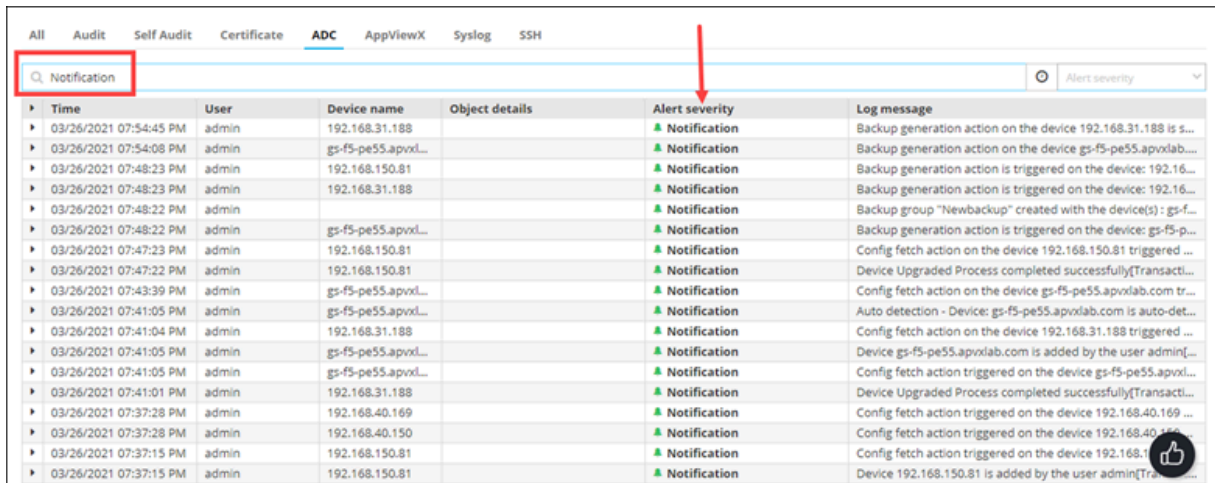
Based on the Values Recorded for each Log

To search for logs based on a value for one of the categories, for example, to search for ADC logs with the severity Notification:

1. Navigate to the **Logging :: ADC** page.
2. From the drop-down menu in the **Search** field, select a category, for example, **Alert Severity**, for searching the required logs.

3. In the **Search** field, enter a search value. for example, **Notification**.

The page is updated to display logs that fulfill the search criteria.



Time	User	Device name	Object details	Alert severity	Log message
03/26/2021 07:54:45 PM	admin	192.168.31.188		Notification	Backup generation action on the device 192.168.31.188 is s...
03/26/2021 07:54:08 PM	admin	gs-f5-pe55.apvxl...		Notification	Backup generation action on the device gs-f5-pe55.apvxl...
03/26/2021 07:48:23 PM	admin	192.168.150.81		Notification	Backup generation action is triggered on the device: 192.16...
03/26/2021 07:48:23 PM	admin	192.168.31.188		Notification	Backup generation action is triggered on the device: 192.16...
03/26/2021 07:48:22 PM	admin			Notification	Backup group "Newbackup" created with the device(s) : gs-f...
03/26/2021 07:48:22 PM	admin	gs-f5-pe55.apvxl...		Notification	Backup generation action is triggered on the device: gs-f5-p...
03/26/2021 07:47:23 PM	admin	192.168.150.81		Notification	Config fetch action on the device 192.168.150.81 triggered ...
03/26/2021 07:47:22 PM	admin	192.168.150.81		Notification	Device Upgraded Process completed successfully[Transacti...
03/26/2021 07:43:39 PM	admin	gs-f5-pe55.apvxl...		Notification	Config fetch action on the device gs-f5-pe55.apvxl.com tr...
03/26/2021 07:41:05 PM	admin	gs-f5-pe55.apvxl...		Notification	Auto detection - Device: gs-f5-pe55.apvxl.com is auto-det...
03/26/2021 07:41:04 PM	admin	192.168.31.188		Notification	Config fetch action on the device 192.168.31.188 triggered ...
03/26/2021 07:41:05 PM	admin	gs-f5-pe55.apvxl...		Notification	Device gs-f5-pe55.apvxl.com is added by the user admin[...
03/26/2021 07:41:05 PM	admin	gs-f5-pe55.apvxl...		Notification	Config fetch action triggered on the device gs-f5-pe55.apvxl...
03/26/2021 07:41:01 PM	admin	192.168.31.188		Notification	Device Upgraded Process completed successfully[Transacti...
03/26/2021 07:37:28 PM	admin	192.168.40.169		Notification	Config fetch action triggered on the device 192.168.40.169 ...
03/26/2021 07:37:28 PM	admin	192.168.40.150		Notification	Config fetch action triggered on the device 192.168.40.150 ...
03/26/2021 07:37:15 PM	admin	192.168.150.81		Notification	Config fetch action triggered on the device 192.168.150.81 ...
03/26/2021 07:37:15 PM	admin	192.168.150.81		Notification	Device 192.168.150.81 is added by the user admin[Tran...

Forwarding Logs

Before logs are purged, AppViewX enables forwarding logs to external servers, like SIEM, that allows for a detailed analysis and, therefore, better identification of problem areas. This gives an advantage when configuring alerts; new alerts can be created to target and resolve the problem areas identified.

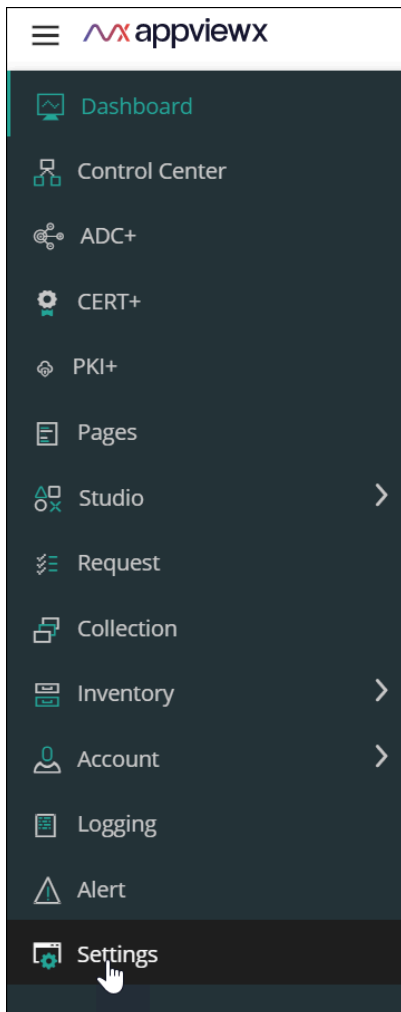
- [Configuring Server Inventory Settings](#)
- [Configuring Forwarding Settings](#)

Configuring Server Inventory Settings

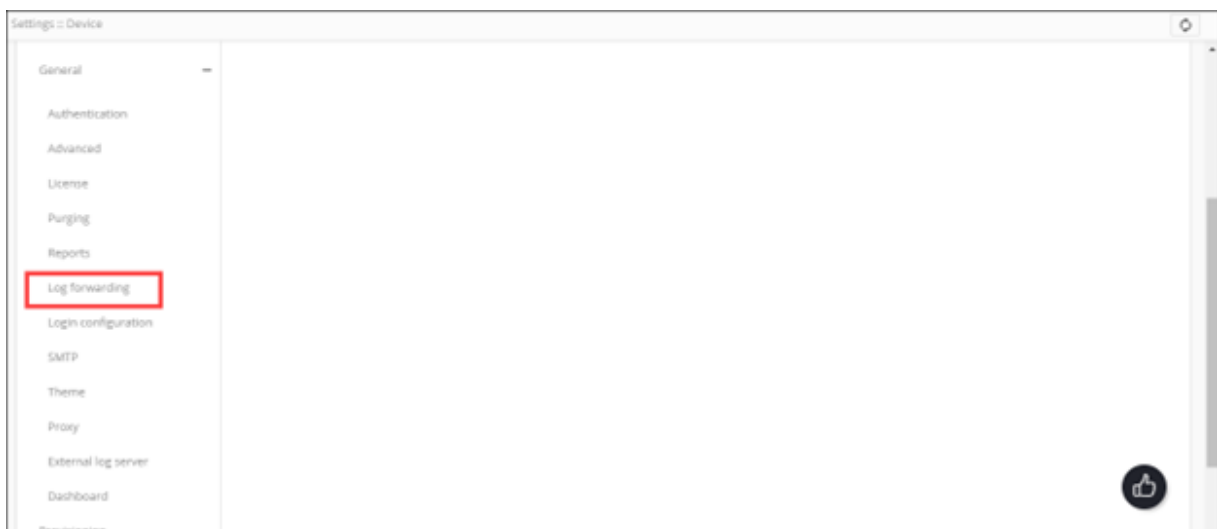
Server inventory settings are used to configure settings for forwarding logs to a specific external server.

To configure server inventory settings:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General** and select **Log Forwarding**.



The **Settings :: Log Forwarding** page is displayed, with the **Server inventory** tab open by default.

Settings :: Log forwarding

Server inventory Forwarding settings

* Server name

* Log server / receiver

Protocol ☐ UDP ☐ TCP ☒ Splunk HEC

* Port

Data center

Enable HTTPS ☐

Index

* Authentication Token

* Log type & severity

☐	Server name	Log server / receiver	Port	Protocol	Log type	Status
☐	asasdas	1.2.3.4	514	UDP	Audit	Enabled
☐	gdsd	1.2.3.5	514	UDP	Audit	Enabled

4. In the **Server inventory** tab, enter the following details (sample values are shown in the image below the table):

Field	Description
*Server name	Name of the external server to which the logs will be forwarded
*Log server / receiver	The IP address of the external server to which the logs will be forwarded
*Protocol	Select a protocol from the following options: • UDP (default) • TCP • Splunk HEC
*Port	Enter the port number to be used for the server.
Data center	From the options available in the dropdown, select the data center.
Enable HTTPS	 Note: This field is enabled if you select Splunk HEC as your Protocol. Enable the HTTPS toggle button if the exposed hostname needs SSL verification.

Field	Description
Index	 Note: This field is enabled if you select Splunk HEC as your Protocol. Enter the IP address or hostname of the server and the index to which logs should be forwarded.
*Authentication Token	 Note: This field is enabled if you select Splunk HEC as your Protocol. Enter the authentication token generated while creating the channel for log forwarding on the server.
*Log type & severity	You can choose to forward logs of a specific type and a specific severity to an external server. To add a log type and severity entry: - From the first drop-down menu, select a log type from the following: • Audit (default) • Certificate • ADC • AppViewX • VisualWorkflow - From the second drop-down menu, select the severity of the log type from the following: • Notification (default) • Debug • Warning • Error • Fatal • Critical  Note: You can select more than one severity value for a log type. To add multiple log types and severity entries:

Field	Description
	a. From the Log type & severity field, click  . b. From the first drop-down menu, select a log type. c. From the second drop-down menu, select a severity for the log type. d. To add another log type and severity entry, repeat steps a to c. To delete a log type and severity entry, from the Log type & severity field, click  .  Note: It is mandatory to have at least one log type and severity entry.
All * marked fields are mandatory.	

5. To save the server inventory settings, click **Save**.

The settings configured in the fields above are displayed in the table shown at the end of the page.

- [Enabling Server Inventory Settings](#)
- [Disabling Server Inventory Settings](#)
- [Deleting Server Inventory Settings](#)

Enabling Server Inventory Settings

To enable a server inventory setting:

1. From the table at the bottom of the **Server inventory** page, select the server inventory setting you want to enable.

☒	Server name	Log server / receiver	Port	Protocol	Log type	Status
☒	UDP	192.168.145.156	5454	UDP	AuditCertificateADCAp...	Enabled

2. From the top right corner of the screen, click .



Note: You can enable multiple server inventory settings by selecting the check box against all the settings you want to enable.

Disabling Server Inventory Settings

To disable a server inventory setting:

1. From the table at the bottom of the **Server inventory** page, select the server inventory setting you want to disable.

☒	Server name	Log server / receiver	Port	Protocol	Log type	Status
☒	UDP	192.168.145.156	5454	UDP	AuditCertificateADCAp...	Enabled

2. From the top right corner of the screen, click .



Note: You can disable multiple server inventory settings by selecting the check box against all the settings you want to disable.

Deleting Server Inventory Settings

To delete a server inventory setting:

1. From the table at the bottom of the **Server inventory** page, select the server inventory setting you want to delete.

☒	Server name	Log server / receiver	Port	Protocol	Log type	Status
☒	UDP	192.168.145.156	5454	UDP	AuditCertificateADCAp...	Enabled

2. From the top right corner of the screen, click .



Note: You can delete multiple server inventory settings by selecting the check box against all the settings you want to delete.

Configuring Forwarding Settings

To configure the forwarding settings follow the below steps:

1. On the **Settings :: Log Forwarding** page, under the **Forwarding settings** tab, enter the following details:

Field	Description
Log format	To select the format in which logs should be forwarded to the external server, from the drop-down menu, select one of the following options: • Syslog • CEF Note: CEF is the most recent industry standard for forwarding logs.
Enable retry	If an attempt to forward logs fails because of server unavailability, AppViewX lets you set a retry interval—the duration after which logs will be forwarded again. To enable this retry, turn on the Enable retry toggle.
*Retry interval	To set a retry interval, from the hour and minutes drop-down menus, select the required values. Note: This field is displayed when the Enable retry toggle is turned on.
All * marked fields are mandatory.	

2. To set a retry interval, from the hour and minutes drop-down menus, select the required values.

Exporting Logs

AppViewX lets you export logs as Excel sheets.

To export logs:

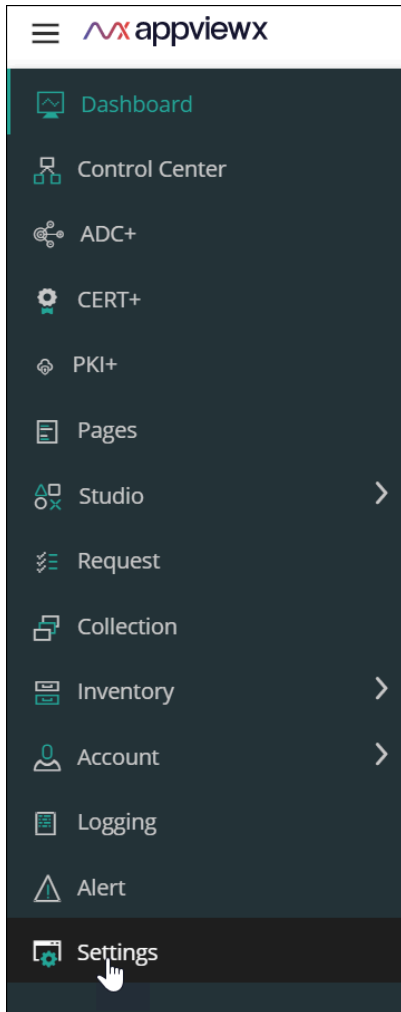
1. Go to the **Logging** page for the log type you want to export.
2. From the top right corner of the **Logging** page, click .
3. Navigate to the location to save the log file and click **Save**.
All logs of the selected log type are downloaded and saved.

Purging Logs

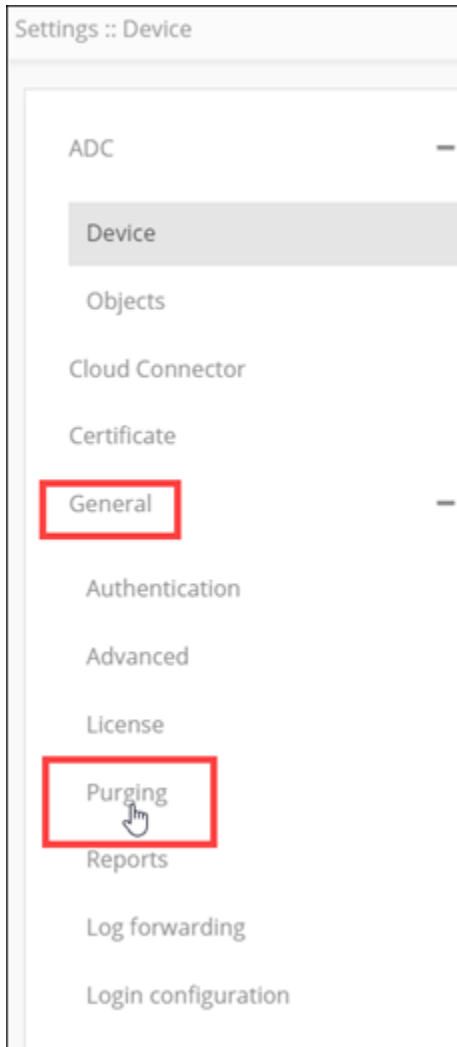
With a large number of log entries being recorded each day, a system can soon become vulnerable to threats like a compromise of confidential information, a surplus of outdated information, and so on. For security reasons, regular purging of old data comes as a highly recommended practice.

To enable purging of log records:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Purging**.



The **Settings :: Purging** screen is displayed.

5. To configure the log purging settings, on the **Settings :: Purging** page, click the **Logging** tab.
6. Under the **Logging** tab, enter the following details:

The screenshot displays the 'Settings :: Purging' interface. On the left is a sidebar with navigation options: ADC, Device, Objects, Cloud Connector, Certificate, General, Authentication, Advanced, License, Purging, and Reports. The 'Purging' option is selected. The main area has two tabs: 'Alert' and 'Logging'. The 'Logging' tab is active, showing two configuration fields: 'Logging Purge Duration(in Days)' with a value of 500 and 'Maximum Logging count' with a value of 3000. Below these fields are 'Save' and 'Cancel' buttons. To the right of the input fields is a 'Note' section with the following text:

Note
When the count value is set to 30,000 and the duration as 50 days.

Count exceeds before duration ends :
If there are 50,000 logs received within 50 days (Duration), the latest 30,000 logs (Count) will be stored and the rest will be purged.

Duration reached before count exceeds :
If the duration limit is reached (50 days) before the count limit (30,000), all logs received during that period will be purged.

Field	Description
*Logging Purge Duration (in Days)	Enter the number of days, the interval, after which logs will be purged.
*Maximum Logging count	Enter the maximum number of the most recent logs that have to be retained. For example, if you set this value to 10,000, all logs after the first 10,000 logs will be purged.
All * marked fields are mandatory.	



Note: Excess logs will be purged even if the maximum logging count is exceeded before the next purging cycle is scheduled.

7. Click **Save**.

Chapter 7: HSM Integration for AppViewX

- [Overview](#)
- [Utimaco](#)
- [Fortanix](#)
- [Thales DPOD](#)
- [Thales GPN](#)

Overview

An HSM (Hardware Security Module) is a piece of hardware and associated software or firmware that usually resides in a PC or server and provides at least the minimal cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The physical device offers physical tamper-resistance and has a user interface and a programmable interface. Other names for an HSM include Personal Computer Security Module (PCSM), Secure Application Module (SAM), Hardware Cryptographic Device, or Cryptographic Module.

For the deployment, AppViewX enables support for integrating all HSMs that support the PKCS11 library, an interface that facilitates interaction between the HSM and AppViewX. This eliminates the need to deploy vendor-specific SDKs and JAR files, thus significantly reducing the time it takes for integrating and installing an HSM.

The deployment currently supports the following four HSM vendors:

- Utimaco
- Fortinax
- Thales - DPOD
- Thales - GPN

Utimaco

To integrate a HSM device from Amazon, enter the following details:

Field	Description
Slot Id*	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device
Partition password*	Password of the HSM partition for the specific slot mentioned above
Key handler name*	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
All * marked fields are mandatory.	

- [Integrating the Utimaco HSM with the AppViewX](#)

Integrating the Utimaco HSM with the AppViewX

To integrate the Utimaco HSM with the AppViewX:

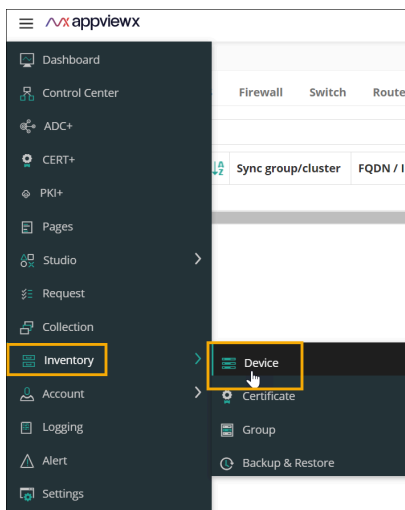
1. Login to the AppViewX server on which the AppViewX Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder. Path:
{CC_INSTALLATION_PATH}/deps/properties
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Uncomment the following lines:

```
export CS_PKCS11_R2_CFG= /appviewx/dependencies/external_libs/hsm/utimaco/cs_pkcs11_R2.cfg
echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"
```

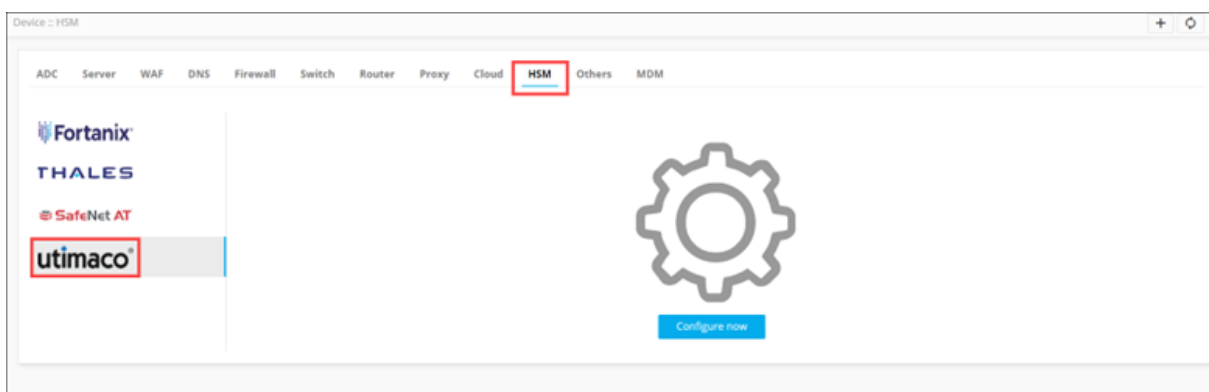
5. Login to the AppViewX UI using valid credentials. B
The **Dashboard** page is displayed by default.
6. From the top-left corner of the page, click .
7. From the menu displayed, select **Inventory > Device**.



The **Device :: ADC** page is displayed.

Name	Sync group/cluster	FQDN / IP address	Port	Version	Status	Vendor	Modules
15056		192.168.150.56	22	1.5.18	Managed	HAProxy	SLB
192.168.142.197		192.168.142.197	22	13.1.3.4 build 0.0.5	Managed	F5	LTM,BIG-IP DNS
192.168.31.189	hasyncfailover	192.168.31.189	22	15.0.1 build 0.0.11	Managed	F5	LTM,BIG-IP DNS
192.168.31.42		192.168.31.42	22	13.0 build 58.32.nc	Managed	Citrix	SLB
192.168.94.6		192.168.94.6	22	1.8.3	Managed	HAProxy	SLB
aws1234_38/84802/138			22		Managed	AmazonELB	
gs-f5-pe115.lab.appviewx.net	ha group	192.168.40.169	22	11.6.3.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS
gs-f5-pe54.apvlab.com	hasyncfailover	192.168.31.188	22	15.0.1 build 0.0.11	Failed	F5	LTM,BIG-IP DNS
test	ha-group	192.168.40.150	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS

8. Under the **HSM** tab, from the navigation pane on the left, select **Utimaco**.



9. Click **Configure now**.

The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX SaaS.

10. In the **General Information** section, enter/select the required field information.

General information

* Name

Description

Implementation type

CSR Generation

▼

Default

Off

* Data center

dc1

▼

The following table describes the field information in this section:

Field	Description
*Name	Enter a name for this integration.
Description	Enter a description for the integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Private key generation • Both
Default	Turn on the toggle to make this the default setting.
*Data center	From the dropdown list, from the list of applicable values, select the required data center.  Note: The data center selected here is used to map the AppViewX Cloud Connector for this integration.
All * marked fields are mandatory.	

11. In the Vendor specific details section, enter/select the required field information.

Vendor specific details

* Slot Id

* Partition password

* Key handler name

* So File

* Config file

The following table describes the field information in this section:

Field	Description
*Slot Id	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.
*Partition password	Password of the HSM partition for the specific slot mentioned above.
*Key handler name	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
*So File	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: - Click Browse. - Navigate to the location of the .so file. - Select the .so file and click Open.
*Config file	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: - Click Browse. - Navigate to the location of the .conf file. - Select the .conf file and click Open.

Field	Description
All * marked fields are mandatory.	

12. Click **Save**.
13. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. If the HSM has been configured correctly, the Status for the HSM will be set to **Available** (after checking the encryption and decryption logic). If the Status is **Not Available**:
 - Check the installation path for the HSM.
 - Ensure that all required permissions have been enabled.
14. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Fortanix

To integrate a HSM device from Amazon, enter the following details:

Field	Description
*API Key	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.
*Key handler name	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
All * marked fields are mandatory.	

- [Integrating the Fortanix HSM with the AppViewX](#)

Integrating the Fortanix HSM with the AppViewX

To integrate the Fortanix HSM with the AppViewX:

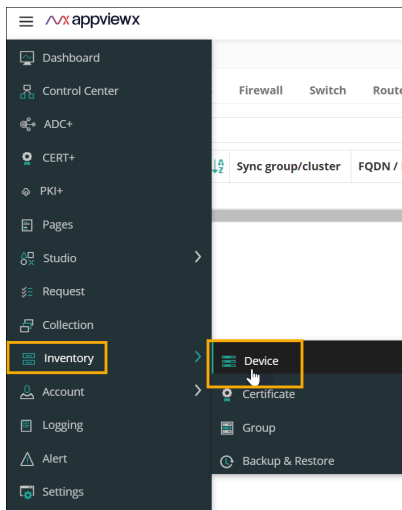
1. Login to the AppViewX server on which the AppViewX Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder. Path:
{CC_INSTALLATION_PATH}/deps/properties
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Uncomment the following lines:

```
export FORTANIX_PKCS11_CONFIG_PATH= /appviewx/dependencies/hsm/fortanix/pkcs11.conf
echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

5. Login to the AppViewX UI using valid credentials.
6. From the top left corner of the screen, click 
7. From the menu displayed, select **Inventory** > **Device**.



The **Device :: ADC** page is displayed.

Device :: ADC								
ADC Server WAF DNS Firewall Switch Router Proxy Cloud HSM Others MDM								
Search...								
☐	Name	Sync group/cluster	FQDN / IP address	Port	Version	Status	Vendor	Modules
☐	15055		192.168.150.56	22	1.5.18	Managed	HAProxy	SLB
☐	192.168.142.197		192.168.142.197	22	13.1.3.4 build 0.0.5	Managed	F5	LTM,BIG-IP DNS
☐	192.168.31.189	hasyncfailover	192.168.31.189	22	15.0.1 build 0.0.11	Managed	F5	LTM,BIG-IP DNS
☐	192.168.31.42		192.168.31.42	22	13.0 build 58.32.nc	Managed	Citrix	SLB
☐	192.168.94.6		192.168.94.6	22	1.8.8	Managed	HAProxy	SLB
☐	aws1234_387848027138			22		Managed	AmazonELB	
☐	gs-fs-pe115.lab.appviewx.net	ha group	192.168.40.169	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS
☐	gs-fs-pe34.apvlab.com	hasyncfailover	192.168.31.188	22	15.0.1 build 0.0.11	Failed	F5	LTM,BIG-IP DNS
☐	test	ha-group	192.168.40.150	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS

8. Under the **HSM** tab, from the navigation pane on the left, select **Fortanix**.

9. Click **Configure now**.

The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX SaaS.

10. In the **General information** section, enter/select the following details:

Field	Description
*Name	Enter a name for this integration.
Description	Enter a description for this integration.
Implementation type	Select an implementation type from the options available in the dropdown menu.
Default	Turn on the toggle to make this the default setting.
*Data center	Select the required data center from the list of applicable values in the dropdown menu.
All * marked fields are mandatory.	

11. In the **Vendor specific details** section, enter/select the following details:

Field	Description
*API Key	Enter the API key.

Field	Description
*Key handler name	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
*So file	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: a. Click Browse . b. Navigate to the location of the .so file. c. Select the .so file and click Open .
*Config file	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: a. Click Browse . b. Navigate to the location of the .conf file. c. Select the .conf file and click Open .
All * marked fields are mandatory.	

12. Click **Save**.
13. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. If the HSM has been configured correctly, the Status for the HSM will be set to **Available** (after checking the encryption and decryption logic). If the Status is **Not Available**:
 - Check the installation path for the HSM.
 - Ensure that all required permissions have been enabled.
14. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Thales DPoD

In this section, you will be guided to integrate the Thales DPoD HSM with the AppViewX SaaS.

- [Integrating the Thales DPoD HSM with the AppViewX](#)

Integrating the Thales DPoD HSM with the AppViewX

To integrate the Thales DPoD HSM with the AppViewX:

1. Login to the AppViewX server on which the AppViewX Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder. Path:
{CC_INSTALLATION_PATH}/deps/properties
3. Open the hsm file, using the following command:

```
vi hsm
```

4. In the **hsm** file, uncomment the following lines:

```
cd /appviewx/dependencies/external_libs/hsm/safenet/dpod/

source setenv

export ChrystokiConfigurationPath=/appviewx/dependencies/hsm/safenet/dpod/
```



Note: The given path is only for reference, if there is change in the installed path the same has to be updated in the above commands.

5. Navigate to the hsm folder. Path: **{installation_path}/deps/external_libs/hsm/**
6. Install the Luna client in this location.



Note: If the Luna client is already installed location, you will have to uninstall and reinstall the Luna client at the location: **{appviewx_installation_path}/hsm/**.

7. Untar the **DPoD** tar file.
8. After successful installation, copy the **Chrystoki.conf** file to the location `cp /etc/Chrystoki.conf {CC_INSTALLATION_PATH}/deps/external_libs/hsm/`.
9. Edit the **Chrystoki.conf** file to replace the custom path with the above new mount path.
10. For version 7.2, enable the folder permissions using the command given below:

```
"cd {appviewx_installation_path}/hsm/safenet/lunaclient"

"sudo find . -type d -exec chmod +rx {} \;"
```

11. Update the permissions for the **Chrystoki.conf** file using the command given below:

```
SaaS : " cd {appviewx_installation_path}/hsm/"

"sudo chmod 755 Chrystoki.conf"
```

AppViewX can now communicate with all HSM devices.

12. Restart the avx-platform-hsm pod, using the following commands:

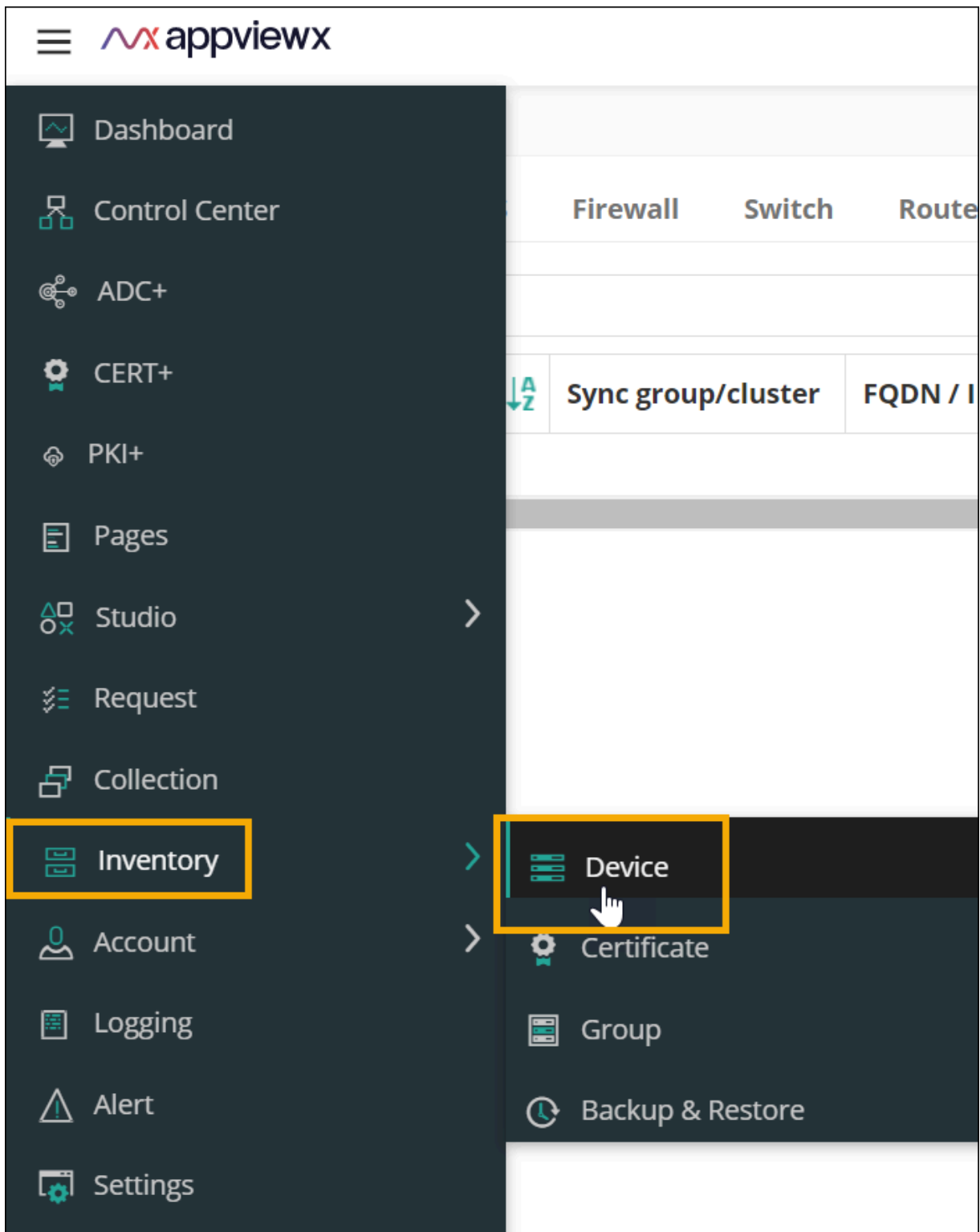
```
list kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

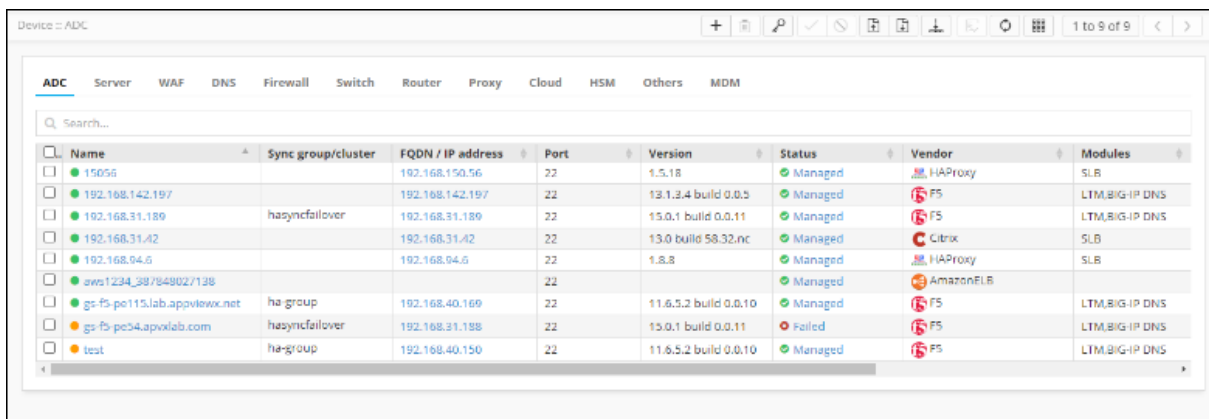
13. Login to the AppViewX UI using valid credentials.

The **Dashboard** page is displayed by default.

14. From the top left corner of the screen, click 
15. From the menu displayed, select **Inventory** > **Device**.



The **Device :: ADC** page is displayed.



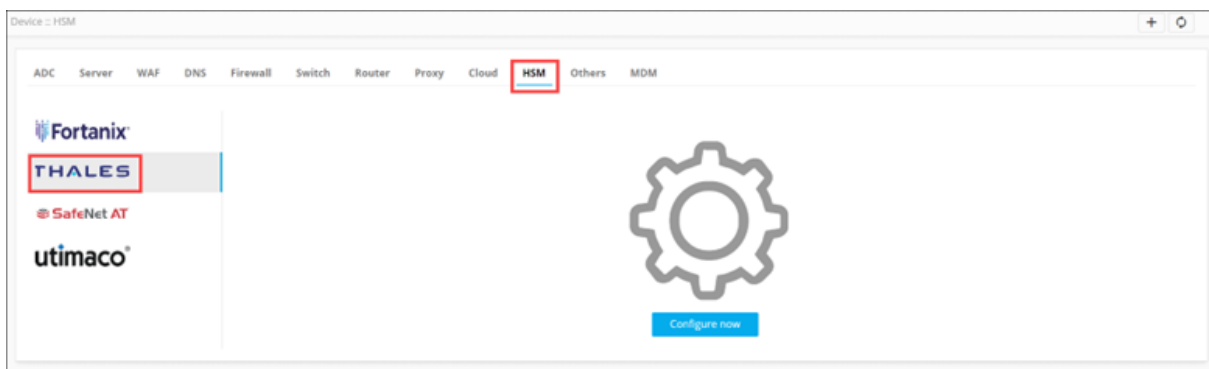
Device :: ADC

ADC Server WAF DNS Firewall Switch Router Proxy Cloud HSM Others MDM

Search...

Name	Sync group/cluster	FQDN / IP address	Port	Version	Status	Vendor	Modules
15056		192.168.150.56	22	1.5.18	Managed	HAProxy	SLB
192.168.142.197		192.168.142.197	22	13.1.3.4 build 0.0.5	Managed	F5	LTM,BIG-IP DNS
192.168.31.189	hasyncfailover	192.168.31.189	22	15.0.1 build 0.0.11	Managed	F5	LTM,BIG-IP DNS
192.168.31.42		192.168.31.42	22	13.0 build 58.32.nc	Managed	Citrix	SLB
192.168.04.6		192.168.04.6	22	1.8.8	Managed	HAProxy	SLB
aws1234_38784802/138			22		Managed	AmazonELB	
gs-f5-pe115.lab.apviewx.net	ha group	192.168.40.169	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS
gs-f5-pe34.apviewx.com	hasyncfailover	192.168.31.188	22	15.0.1 build 0.0.11	Failed	F5	LTM,BIG-IP DNS
test	ha-group	192.168.40.150	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS

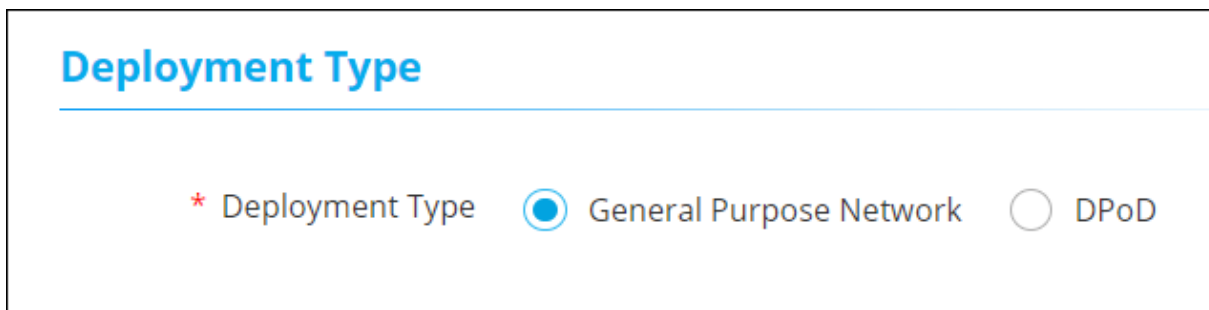
16. Under the **HSM** tab, from the navigation pane on the left, select **Thales**.



17. Click **Configure now**.

The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX SaaS.

18. In the **Deployment Type** section, for the **Deployment Type** field, select **General Purpose Network**.



Deployment Type

* Deployment Type ☒ General Purpose Network ☐ DPoD

19. In the **General Information** section, enter/select the required field information.

General information

* Name

Description

Implementation type

CSR Generation

▼

Default

Off

* Data center

dc1

▼

The following table describes the field information in this section:

Field	Description
*Name	Enter a name for this integration.
Description	Enter a description for the integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Private key generation • Both
Default	Turn on the toggle to make this the default setting.
*Data center	From the dropdown list, from the list of applicable values, select the required data center.  Note: The data center selected here is used to map the AppViewX Cloud Connector for this integration.
All * marked fields are mandatory.	

20. In the **Vendor specific details** section, enter/select the required field information.

Vendor specific details

* Slot Id

* Partition password

* Key handler name

* So File

* Config file

The following table describes the field information in this section:

Field	Description
*Slot Id	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.
*Partition password	Password of the HSM partition for the specific slot mentioned above.
*Key handler name	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
*So File	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: - Click Browse. - Navigate to the location of the .so file. - Select the .so file and click Open.
*Config file	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: - Click Browse. - Navigate to the location of the .conf file. - Select the .conf file and click Open.

Field	Description
All * marked fields are mandatory.	

21. Click **Save**.
22. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. If the HSM has been configured correctly, the Status for the HSM will be set to **Available** (after checking the encryption and decryption logic). If the Status is **Not Available**:
 - Check the installation path for the HSM.
 - Ensure that all required permissions have been enabled.
23. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Thales GPN

In this section, you will be guided to integrate the Thales GPN HSM with the AppViewX SaaS.

- [Installing the Luna Client](#)
- [Integrating the Thales GPN HSM with the AppViewX](#)

Installing the Luna Client

In order to communicate with the HSM in the customers' premises, install the Luna client on the node where the AppViewX Cloud Connector is installed.

Prerequisites

- The Alien and RPM packages should be installed in the environment.
- Users should have either root access or sudo access.
- Environment should have access to communicate with HSM through the ports 22, 1792.

Integrating the Thales GPN HSM with the AppViewX

1. Login to the AppViewX server on which the AppViewX Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder. Path:
{CC_INSTALLATION_PATH}/deps/properties
3. Open the hsm file using the following command:

```
vi hsm
```

4. In the hsm file, uncomment the following lines:

```
export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/
```



Note: The given path is only for reference, if there is change in the installed path the same has to be updated in the above commands.

5. Navigate to the hsm folder. Path: `{APPVIEWX_INSTALLATION_PATH}/hsm/`

6. Install the Luna client in this location.



Note: If the Luna client is already installed location, you will have to uninstall and reinstall the Luna client at the location: `{AppViewX_installed_path}_deps/external_lib/hsm/`

7. After successful installation, copy the **Chrystoki.conf** file to the location `cp /etc/Chrystoki.conf`

```
{CC_INSTALLATION_PATH}/deps/external_libs/hsm/.
```

8. Edit the **Chrystoki.conf** file to replace the custom path with the above new mount path.

9. For version 7.2, enable the folder permissions using the command given below:

```
"cd {AppViewX_INSTALLATION_PATH}/hsm/safenet/lunaclient"
"sudo find . -type d -exec chmod +rx {} \;"
```

10. Update the permissions for the **Chrystoki.conf** file using the command given below:

```
SaaS : " cd {AppViewX_INSTALLATION_PATH}/hsm/"
"sudo chmod 755 Chrystoki.conf"
```

AppViewX can now communicate with all HSM devices.

11. Restart the avx-midserver-platform pod, using the following commands:

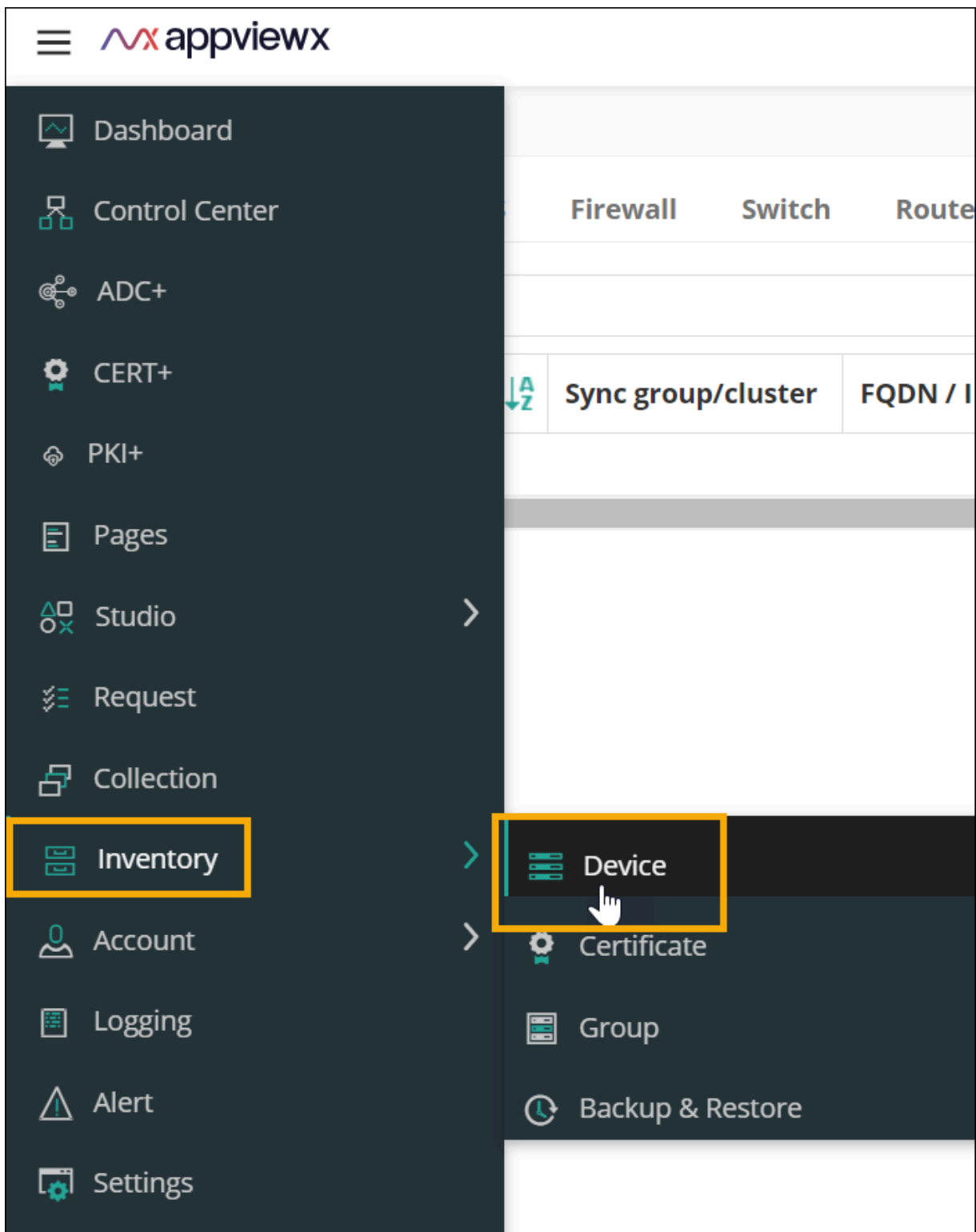
```
list kubectl get pods -n <namespace>
kubectl delete pods -n <namespace> <PodName>
```

12. Login to the AppViewX UI using valid credentials.

The **Dashboard** page is displayed by default.

13. From the top-left corner of the page, click .

14. From the menu displayed, select **Inventory > Device**.



The **Device :: ADC** page is displayed.

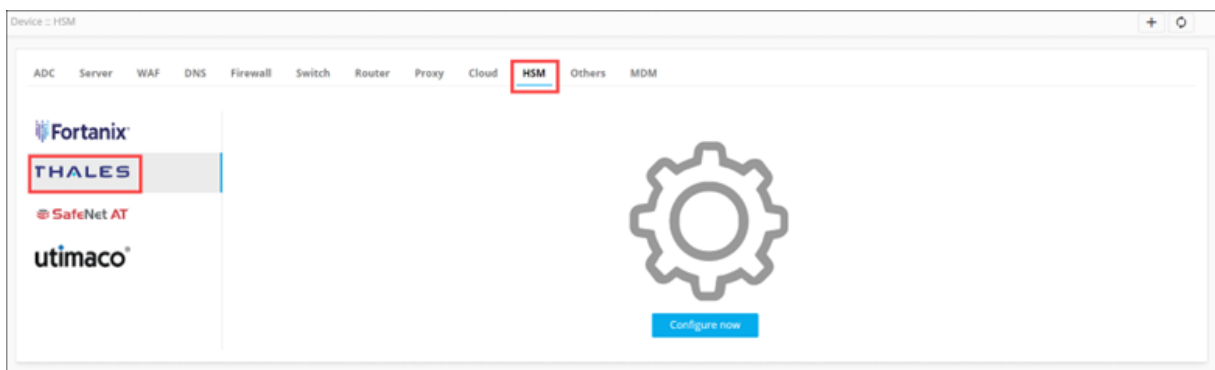
Device :: ADC

ADC Server WAF DNS Firewall Switch Router Proxy Cloud HSM Others MDM

Search...

Name	Sync group/cluster	FQDN / IP address	Port	Version	Status	Vendor	Modules
15059		192.168.150.56	22	1.5.18	Managed	HAProxy	SLB
192.168.142.197		192.168.142.197	22	13.1.3.4 build 0.0.5	Managed	F5	LTM,BIG-IP DNS
192.168.31.189	hasyncfailover	192.168.31.189	22	15.0.1 build 0.0.11	Managed	F5	LTM,BIG-IP DNS
192.168.31.42		192.168.31.42	22	13.0 build 58.32.nc	Managed	Citrix	SLB
192.168.94.6		192.168.94.6	22	1.8.8	Managed	HAProxy	SLB
aws1234_387848027138			22		Managed	AmazonELB	
gs-f5-pe115.lab.apviewx.net	ha group	192.168.40.169	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS
gs-f5-pe34.apvlab.com	hasyncfailover	192.168.31.188	22	15.0.1 build 0.0.11	Failed	F5	LTM,BIG-IP DNS
test	ha-group	192.168.40.150	22	11.6.5.2 build 0.0.10	Managed	F5	LTM,BIG-IP DNS

15. Under the **HSM** tab, from the navigation pane on the left, select **Thales**.



16. Click **Configure now**.

The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX SaaS.

17. In the **Deployment Type** section, for the **Deployment Type** field, select **General Purpose Network**.

Deployment Type

* Deployment Type ☒ General Purpose Network ☐ DPoD

18. In the **General Information** section, enter/select the required field information.

General information

* Name

Description

Implementation type

CSR Generation

▼

Default

Off

* Data center

dc1

▼

The following table describes the field information in this section:

Field	Description
*Name	Enter a name for this integration.
Description	Enter a description for the integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Private key generation • Both
Default	Turn on the toggle to make this the default setting.
*Data center	From the dropdown list, from the list of applicable values, select the required data center.  Note: The data center selected here is used to map the AppViewX Cloud Connector for this integration.
All * marked fields are mandatory.	

19. In the Vendor specific details section, enter/select the required field information.

Vendor specific details

* Slot Id

* Partition password

* Key handler name

* So File

* Config file

The following table describes the field information in this section:

Field	Description
*Slot Id	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.
*Partition password	Password of the HSM partition for the specific slot mentioned above.
*Key handler name	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
*So File	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: - Click Browse. - Navigate to the location of the .so file. - Select the .so file and click Open.
*Config file	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: - Click Browse. - Navigate to the location of the .conf file. - Select the .conf file and click Open.

Field	Description
All * marked fields are mandatory.	

20. Click **Save**.
21. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. If the HSM has been configured correctly, the Status for the HSM will be set to **Available** (after checking the encryption and decryption logic). If the Status is **Not Available**:
 - Check the installation path for the HSM.
 - Ensure that all required permissions have been enabled.
22. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Chapter 8: Managing Alerts

- [Overview](#)
- [Viewing Existing Alerts](#)
- [Setting the Record Count Preference for Viewing Alerts](#)
- [Configuring Alerts](#)
- [Editing Alerts](#)
- [Deleting Alerts](#)
- [Searching for Alerts](#)
- [Purging Alerts](#)

Overview

Alert management is important for an organization to monitor and respond to security concerns before they become a threat to the organization's security.

As part of its alert management, AppViewX enables you to identify complications that may occur within an application. Alerts can then be configured, to notify the users of these complications, and send a predetermined date and time using email and SNMP configurations.

AppViewX enables managing alerts in the following categories:

Alert type	Description
Certificate	Alerts triggered when a certificate is invalid, about to expire, or out of sync
SSH	Alerts related to SSH components
ADC	ADC alerts for changes that are triggered through AppViewX
AppViewX	Alerts related to AppViewX-specific components
Syslog	Syslog alerts of critical applications and devices for changes that are executed on the device and

For each alert type, AppViewX defines the following severity levels:

Severity level	Description
Critical	Alerts for issues that can disastrously impact functionality are marked as critical alerts. These are resolved immediately.
Fatal	Alerts for issues that can disastrously impact functionality are marked as fatal alerts. These are resolved immediately.
Major	Alerts for issues that are important and require a resolution, but are not a top priority, are marked as major alerts.
Minor	Alerts for issues that are low priority are marked as minor alerts.
Notification	Alerts for issues that users have to only be notified/warned of are marked as notifications.

For these alerts, AppViewX lets you:

- View alerts
- Configure alerts
- Search for alerts
- Purge alerts
- Delete alerts

Viewing Existing Alerts

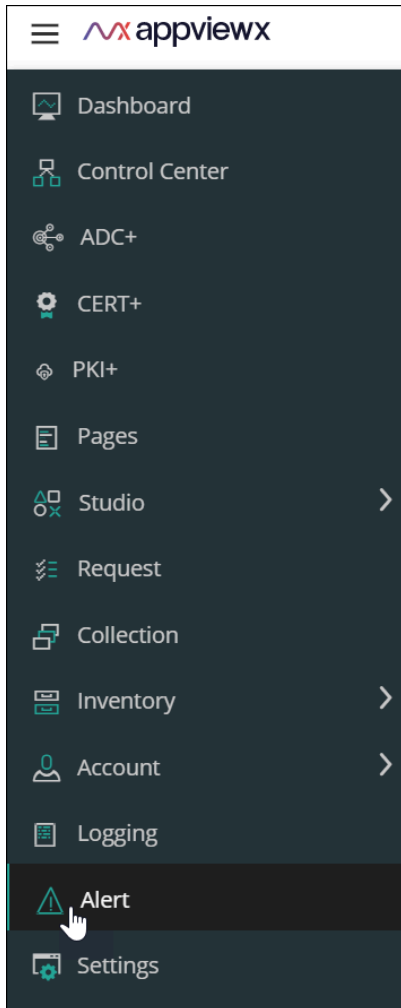
AppViewX lets you view all alerts in one place as well as groups them under the above mentioned categories for a segregated viewing.

- [Viewing All Alerts](#)
- [Viewing AppViewX Alerts](#)
- [Viewing Certificate Alerts](#)
- [Viewing SSH Alerts](#)
- [Viewing Syslog Alerts](#)

Viewing All Alerts

To view all existing alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

Alert :: All 1 to 100 of 6,676

All Certificate SSH ADC AppViewX Syslog

Search...

Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 01:...	Alert_005658	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005657	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005656	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005655	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005654	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005653	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005652	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005651	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005650	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005649	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005648	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005647	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005646	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005645	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005644	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005643	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005642	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005641	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005640	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

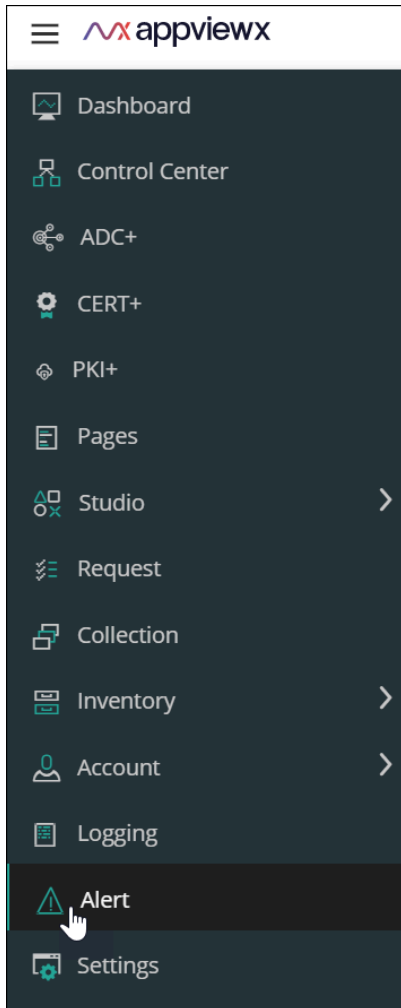
For each alert, this page displays the following details:

Field	Description
Time stamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

Viewing AppViewX Alerts

To view the AppViewX alerts:

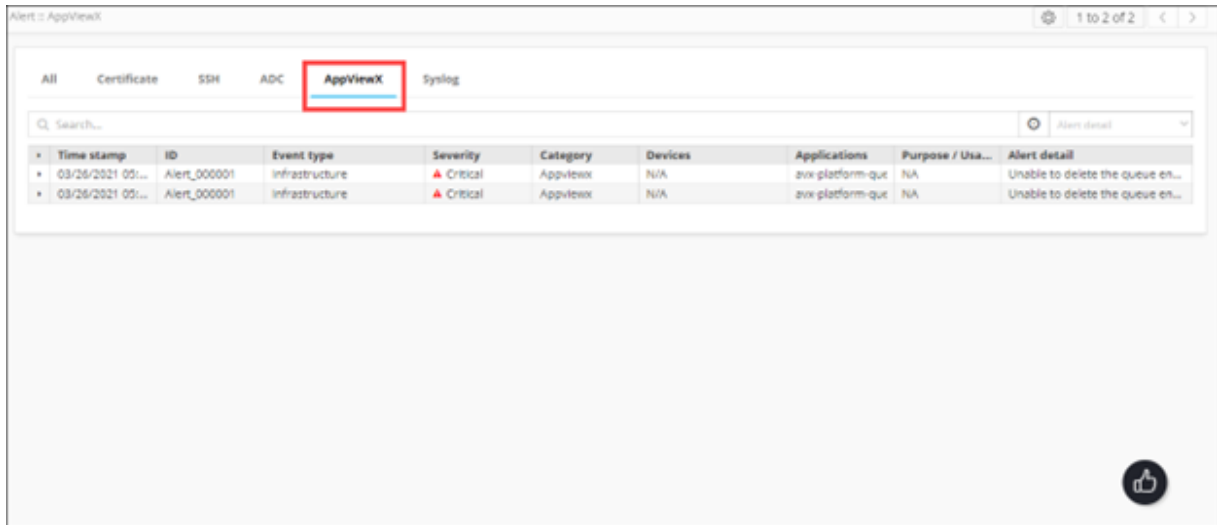
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

3. On the **Alert :: All** page, click the **AppViewX** tab.

The **Alert :: AppViewX** page is displayed.



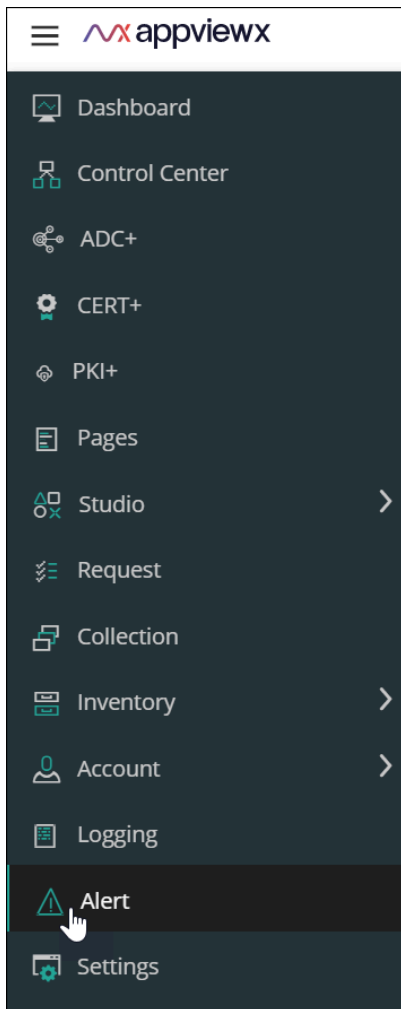
For the AppViewX alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

Viewing Certificate Alerts

To view the Certificate alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

3. On the **Alert :: All** page, click the **Certificate** tab.

The **Alert :: Certificate** page is displayed.

Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 03:...	Alert_006489	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006488	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006487	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006486	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006485	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006484	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006483	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006482	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006481	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006480	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006480	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006479	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006478	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006477	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006476	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006475	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006474	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 03:...	Alert_006473	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

For the Certificate alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

Viewing SSH Alerts

To view the SSH alerts:

1. On the Alert page, click the SSH tab.

Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Usa...	Alert detail
03/19/2021 03:...	Alert_006350	SSH Host alert	Major	SSH	192.168.94.6	NA	NA	Host with 192.168.94.6 has be...
03/19/2021 03:...	Alert_006347	SSH Host alert	Major	SSH	192.168.94.6	NA	NA	Host with 192.168.94.6 has be...
03/19/2021 03:...	Alert_006310	SSH Host alert	Major	SSH	192.168.94.6	NA	NA	Host with 192.168.94.6 has be...
03/19/2021 01:...	Alert_005529	SSH Host alert	Major	SSH	192.168.40.214	NA	NA	Host deletion from AppviewX ...
03/19/2021 12:...	Alert_004757	SSH Host alert	Major	SSH	gs-f5-pe15.lab.appview...	NA	NA	Host with gs-f5-pe15.lab.appvi...
03/19/2021 05:...	Alert_002998	SSH Host alert	Major	SSH	gs-f5-pe15.lab.appview...	NA	NA	Host with gs-f5-pe15.lab.appvi...
03/19/2021 05:...	Alert_002998	SSH Host alert	Major	SSH	gs-f5-pe15.lab.appview...	NA	NA	Host with gs-f5-pe15.lab.appvi...
03/18/2021 07:...	Alert_000592	SSH Host alert	Major	SSH	gs-f5-pe15.lab.appview...	NA	NA	Host with gs-f5-pe15.lab.appvi...
03/18/2021 07:...	Alert_000541	SSH Host alert	Major	SSH	192.168.40.152	NA	NA	Host with 192.168.40.152 has ...
03/18/2021 05:...	Alert_000468	SSH Host alert	Major	SSH	192.168.42.150	NA	NA	Host with 192.168.42.150 has ...
03/18/2021 05:...	Alert_000439	SSH Host alert	Major	SSH	192.168.40.214	NA	NA	Host with 192.168.40.214 has ...
03/18/2021 11:...	Alert_000192	SSH Host alert	Major	SSH	192.168.41.251	NA	NA	Host with 192.168.41.251 has ...

2. For the SSH alerts, the page displays the following details:

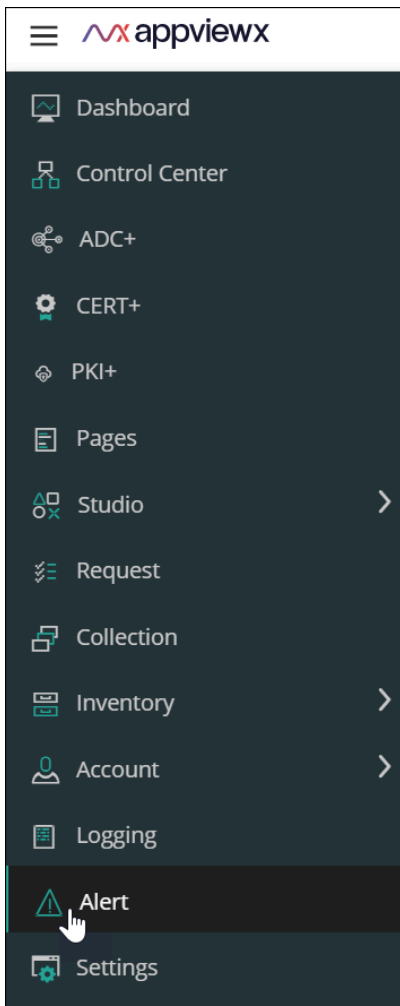
Field	Description
Time stamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID.
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.

Field	Description
Applications	Application that triggered the alert.
Purpose/Usage	The purpose or usage of the alert.
Alert detail	Description of the alert.

Viewing Syslog Alerts

To view the Syslog alerts:

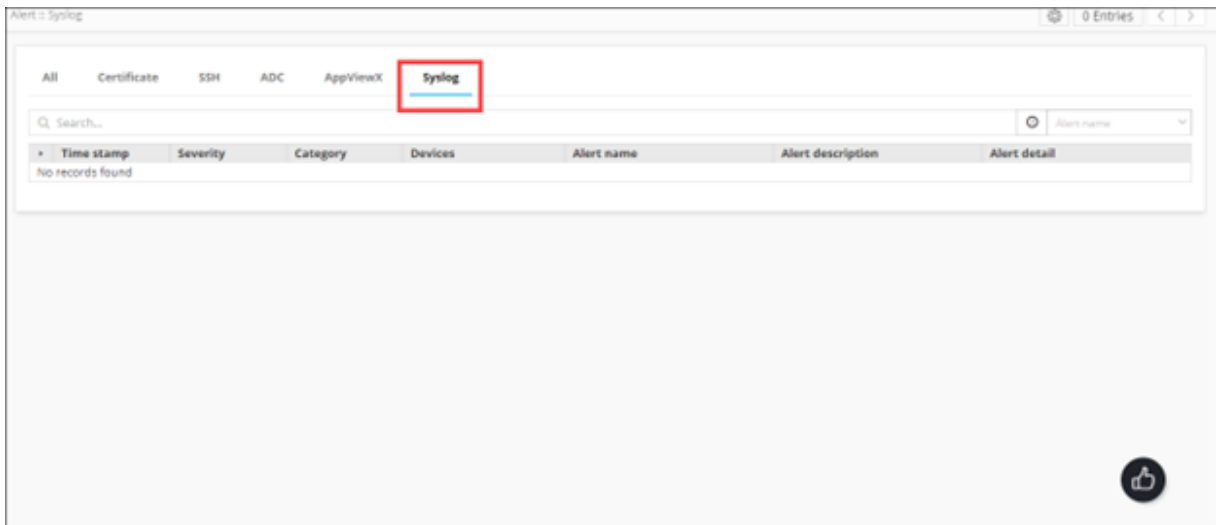
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

- On the **Alert :: All** page, click the **Syslog** tab.

The **Alert :: Syslog** page is displayed.



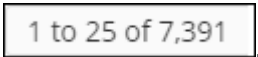
For the Syslog alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

Setting the Record Count Preference for Viewing Alerts

For easier viewing of records, AppViewX lets you set the record count preference, which is the number of alert records that will be displayed on one page.

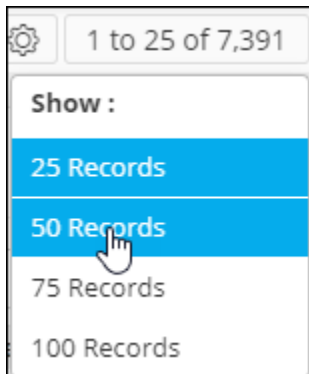
To set the record count preference:

1. On the **Alert :: All** page, from the top-right corner of the screen, click .

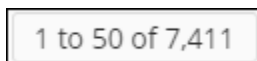


Note: By default, 25 alert records are displayed on one page (which is why the control reads 1 to 25).

2. From the **Show** menu displayed, select your record count preference (for example, 50 records).



3. The Alert page is updated according to the record count preference selected. A message, **Record count preference saved successfully**, is displayed. The UI control is also updated to display the current selection, as shown in the following image:



Configuring Alerts

AppViewX lets you configure alerts to define when the event type that will trigger an alert, the severity of the alert, the message to describe the alert, settings for sending alert notifications, and so on. The subsequent sections outline the instructions for configuring the following types of alerts:

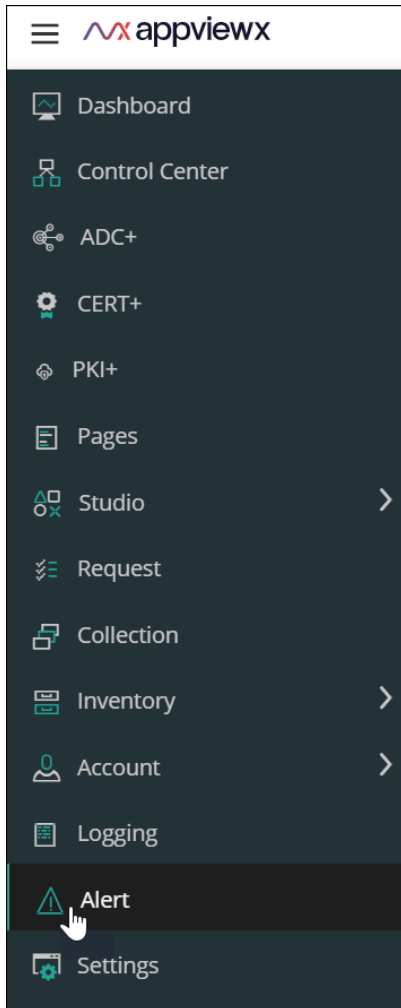
- Certificate
- Syslog

- SSH
- AppViewX
- ADC
- [Configuring ADC Alerts](#)
- [Configuring AppViewX Alerts](#)
- [Configuring Certificate Alerts](#)
- [Configuring SSH Alerts](#)
- [Configuring Syslog Alerts](#)

Configuring ADC Alerts

To configure ADC alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

Alert :: All 1 to 100 of 6,676

All Certificate SSH ADC AppViewX Syslog

Search...

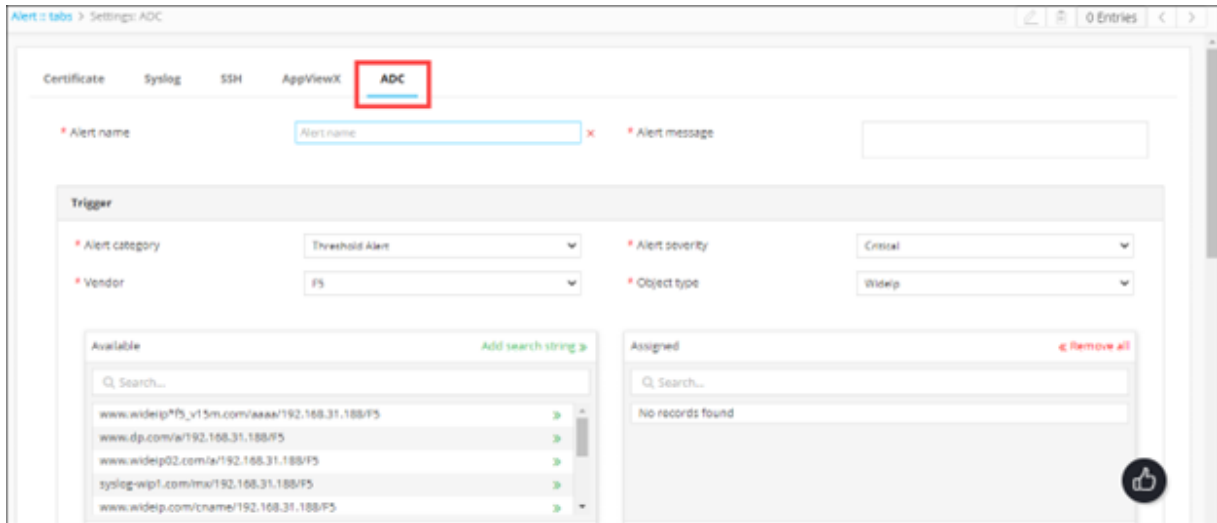
Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 01:...	Alert_005658	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005657	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005656	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005655	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005654	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005653	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005652	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005651	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005650	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005649	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005648	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005647	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005646	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005645	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005644	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005643	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005642	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005641	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005640	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

3. From the top-right corner of the screen, click .

The **Settings :: Certificate** page is displayed.

4. To configure ADC alerts, click **ADC**.

The **Settings :: ADC** page is displayed.



The screenshot shows the 'Settings :: ADC' configuration page. At the top, there are tabs for 'Certificate', 'Syslog', 'SSH', 'AppViewX', and 'ADC', with 'ADC' being the active tab. Below the tabs, there are input fields for 'Alert name' and 'Alert message'. The 'Trigger' section contains four dropdown menus: 'Alert category' (set to 'Threshold Alert'), 'Vendor' (set to 'FS'), 'Alert severity' (set to 'Critical'), and 'Object type' (set to 'Wipe'). Below these, there are two sections: 'Available' and 'Assigned'. The 'Available' section has a search bar and a list of search strings with green arrows next to them. The 'Assigned' section has a search bar and a message 'No records found'.

5. Enter the following details:

Field	Description
*Alert name	Enter the name you want to give this alert.
*Alert message	Enter the message that will be displayed with this alert.
All * marked fields are mandatory.	

6. In the **Trigger** section, enter the following details:

Field	Description
*Alert category	From the drop-down menu, select one of the following alert categories: • Threshold alert • Application alert • Device alert
*Alert severity	From the drop-down, from the options given below, select a severity for the alert: • Critical • Fatal • Major

Field	Description
	• Minor • Notification
Vendor	From the drop-down menu, select the vendor whose device or devices you want to set an alert for.
Object type	From the drop-down menu, select the vendor object that you want to set an alert for.  Note: The contents of this field will vary depending on the vendor selected.
Detail contains	 Note: This field is applicable only for the Device Alert category.
Available	Depending on the Object type and Vendor selected, a list of all available ADC objects or devices is displayed here. To add an object/device to the alert, click  for that object/device.
Add search string	Instead of adding devices manually, AppViewX lets you automatically assign all existing devices or objects that match your criteria. To do this: - In the Available section, in the Search field, enter the search criteria. - Click Add search string.  Note: The benefit of using a search string rather than selecting devices manually is that the search string continues to work in the background and auto-assigns all new devices that match the search criteria.
Assigned	To add an object to the Assigned column, click the check box corresponding to that object.

7. In the **Alert condition** section, enter the following details:

Field	Description
*Alert interval	From the drop-down menu, from the following options, select how often you want the system to check for breaches of the threshold levels that you are about to define:

Field	Description
	• 10 seconds • 20 seconds • 30 seconds • 40 seconds • 50 seconds • 60 seconds
*Cool off period	From the drop-down menu, from the following options, select how much time the system should wait before sending another alert about a continuing threshold breach: • 10 minutes • 20 minutes • 30 minutes
All * marked fields are mandatory.	



Note: This section is applicable only for the Threshold Alert category.

- In the **Statistics** section, define the conditions that will generate an alert by selecting values in the Statistics, Operator, and Value fields.
 - To add more than one Statistics conditions, click .
 - To delete a condition, click .
- In the **Action** section, to send the syslog alert as an email, execute the steps for configuring SMTP for email alerting.
- Enter the following details:

Field	Description
Email configuration	To send the syslog alert as an email, select this check box.
*Email address	To send the syslog alert as an email, enter the email address to which this specific syslog alert will be sent.  Note: Separate multiple email addresses with a comma.
Subject	To send the syslog alert as an email, enter a subject line.
All * marked fields are mandatory.	

11. To use the Simple Network Management Protocol (SNMP) to send the alert, enter the following details:

Field	Description
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
*Destination IP	Enter the destination IP address for the alert.
*Version	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2
*Port	Enter the port number to be used for the alert.
*Community string	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.
All * marked fields are mandatory.	

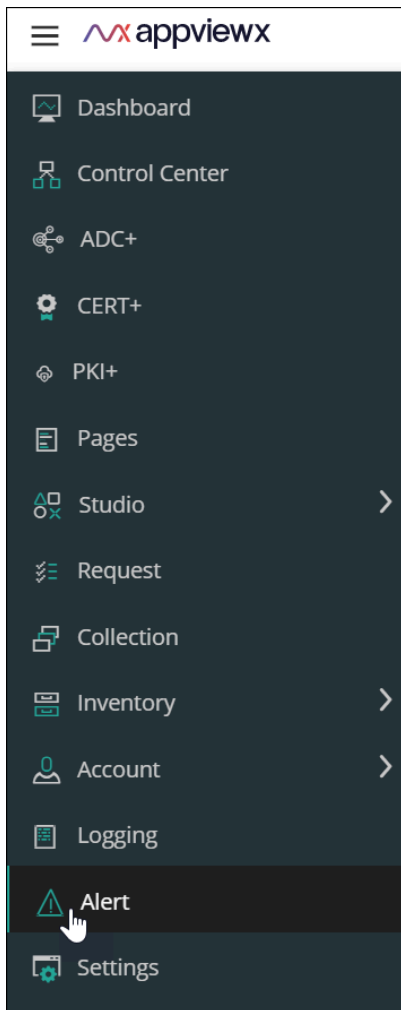
12. To save the ADC alert configure above, click **Add**.

The saved details are displayed in the table shown at the bottom of the screen.

Configuring AppViewX Alerts

To configure AppViewX alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

Alert :: All

1 to 100 of 6,676

All Certificate SSH ADC AppViewX Syslog

Search...

Alert detail

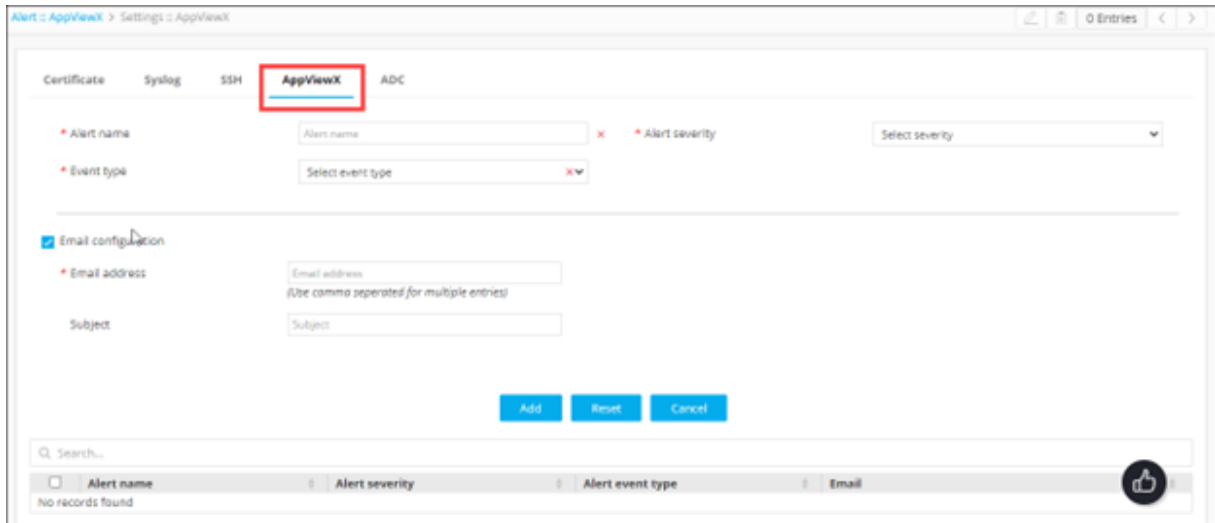
Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 01:...	Alert_005658	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005657	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005656	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005655	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005654	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005653	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005652	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005651	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005650	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005649	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005648	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005647	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005646	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005645	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005644	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005643	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005642	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005641	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005640	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

3. From the top-right corner of the screen, click .

The **Settings :: Certificate** page is displayed.

4. To configure AppViewX alerts, click the AppViewX tab.

The **Settings :: AppViewX** page is displayed.



The screenshot shows the 'Settings :: AppViewX' configuration page. The 'AppViewX' tab is highlighted with a red box. The page includes the following fields and controls:

- Alert name:** A text input field with a red asterisk indicating it is required.
- Alert severity:** A dropdown menu with a red asterisk indicating it is required.
- Event type:** A dropdown menu with a red asterisk indicating it is required.
- Email configuration:** A checked checkbox.
- Email address:** A text input field with a red asterisk indicating it is required. A note below the field says '(Use comma separated for multiple entries)'.
- Subject:** A text input field.

At the bottom of the form are three buttons: 'Add', 'Reset', and 'Cancel'. Below the form is a table with columns: 'Alert name', 'Alert severity', 'Alert event type', and 'Email'. The table shows 'No records found'.

5. Enter the following details:

Field	Description
*Alert name	Enter the name you want to give this alert.
*Alert severity	From the drop-down menu, select a severity for the alert from the following options: • Critical • Fatal • Major • Minor • Notification
*Event type	From the drop-down menu, from the following options, select the event type that will trigger this alert: • Infrastructure • Application Discovery
Email configuration	To send the certificate alert as an email, select this check box.  Note: For AppViewX alerts, this feature is enabled by default.

Field	Description
*Email address	To send the certificate alert as an email, enter the email address to which this specific certificate alert will be sent.  Note: Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.
All * marked fields are mandatory.	

6. To save the alert to the AppViewX system, click **Add**.

The saved details are displayed in the table shown at the bottom of the screen.

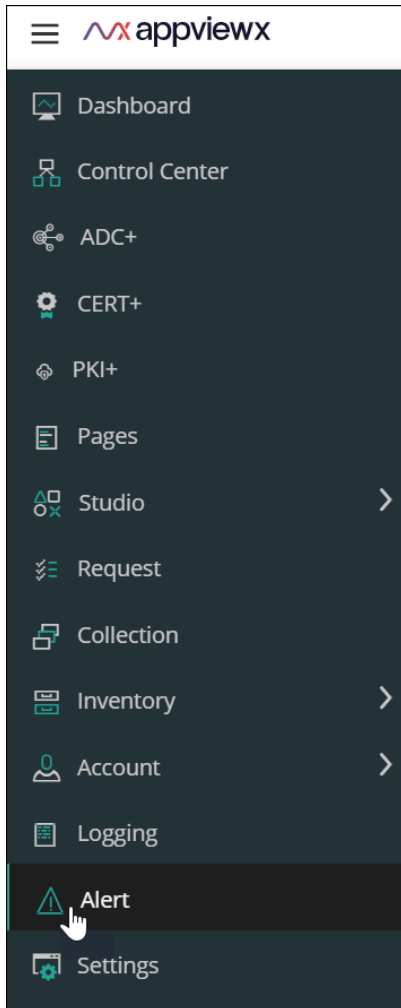
Configuring Certificate Alerts

Certificate alerts are generated to notify users of certificate events that require the user to take a remedial action. Certificate alerts are sent when:

- Certificates need to be validated
- Certificates are set to expire
- Certificates cannot be synchronized

To configure certificate alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

Alert :: All 1 to 100 of 6,676

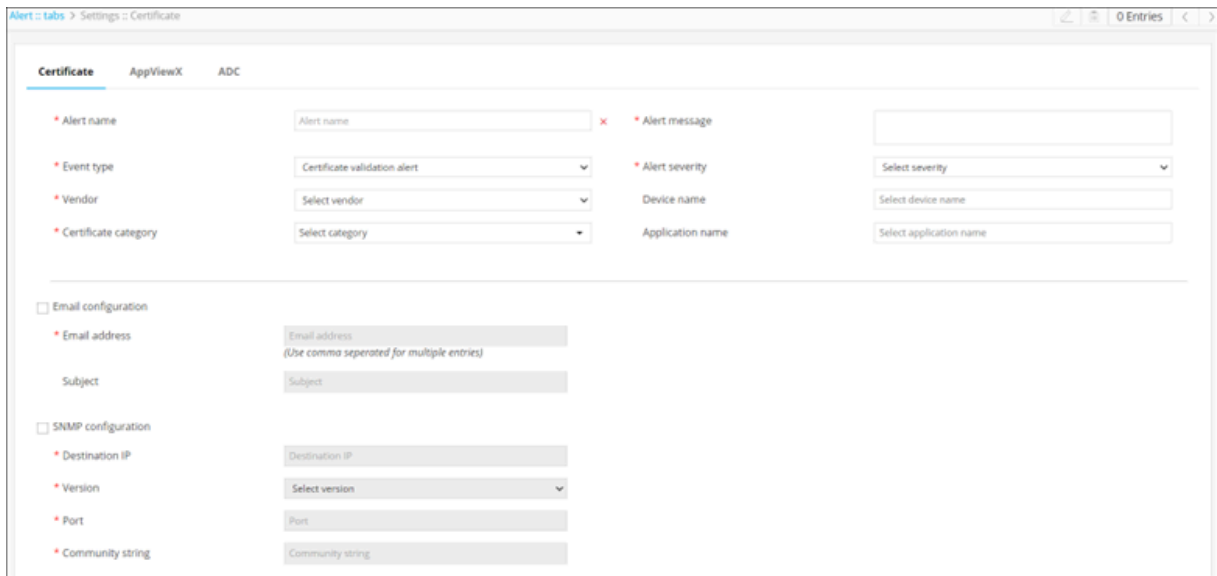
All Certificate SSH ADC AppViewX Syslog

Search...

Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 01:...	Alert_005658	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005657	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005656	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005655	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005654	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005653	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005652	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005651	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005650	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005649	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005648	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005647	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005646	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005645	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005644	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005643	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005642	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005641	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005640	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

3. From the top-right corner of the screen, click .

4. The **Settings :: Certificate** page is displayed, with the **Certificate** tab open by default.



5. To configure certificate alerts, enter the following details:

Field	Description
*Alert name	Enter the name you want to give this alert.
*Alert message	Enter the message that will be displayed with the alert, to describe the alert.  Note: This field is not displayed when configuring the certificate expiry alert.  Note: The alert message cannot be longer than 64 words.
*Event type	From the drop-down menu, select the event type that will trigger this alert from the following options: • Certificate validation alert (default) • Certificate expiry alert • Certificate sync alert
*Alert severity	From the drop-down menu, select a severity for the alert from the following options:

Field	Description
	• Critical • Major • Notification
Vendor	From the drop-down menu, select the vendor name for whose device/application you are creating the alert.  Note: This field is not displayed when configuring the certificate expiry alert.
Device name	Enter the name of the device associated with the certificate you are creating the alert for.  Note: This field is not displayed when configuring the certificate expiry alert.
*Certificate category	From the drop-down menu, select a certificate category from the following options: • Server • Client • Device • Code Signing
*Expires in (days)	Enter the number of days till the certificate expires.  Note: This field is displayed only when configuring certificate expiry alerts.
Email configuration	To send the certificate alert as an email, select this check box.
*Email address	To send the certificate alert as an email, enter the email address to which this specific certificate alert will be sent.  Note: Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.

Field	Description
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
*Destination IP	Enter the destination IP address for the alert.
*Version	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2
*Port	Enter the port number to be used for the alert.
*Community string	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.
All * marked fields are mandatory.	

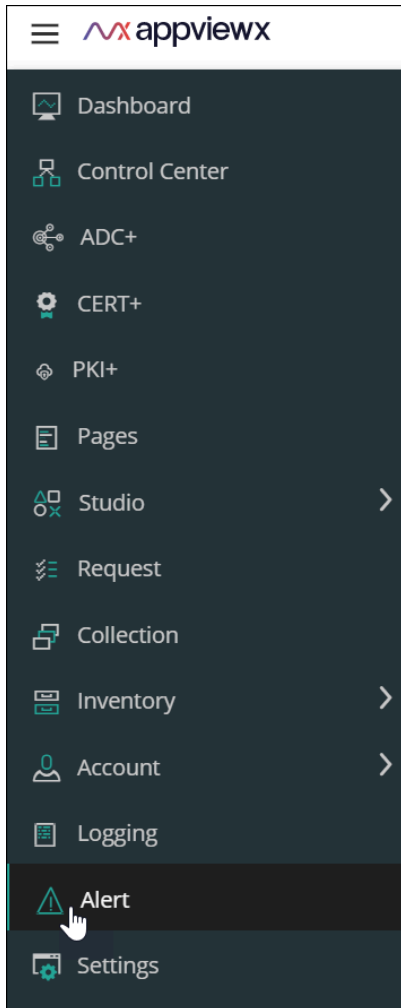
6. To save the certificate alerts configuration details, click **Add**.

The saved details are displayed in the table shown at the bottom of the screen.

Configuring SSH Alerts

To configure syslog alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

Alert :: All

1 to 100 of 6,676

All Certificate SSH ADC AppViewX Syslog

Search...

Alert detail

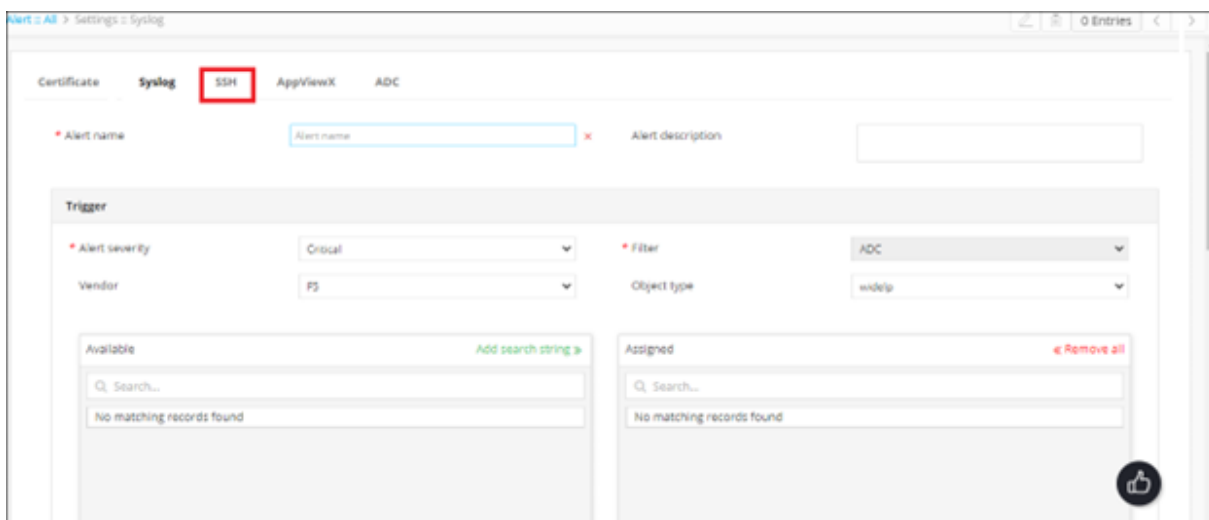
Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 01:...	Alert_005658	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005657	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005656	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005655	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005654	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005653	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005652	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005651	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005650	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005649	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005648	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005647	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005646	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005645	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005644	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005643	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005642	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005641	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005640	Failed to validate revoca...	Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

3. From the top-right corner of the screen, click .

The **Settings :: Certificate** page is displayed.

4. To configure SSH alerts, click **SSH**.

The **Settings :: SSH** page is displayed.



5. Enter the following details:

Field	Description
*Alert name	Enter the name you want to give this alert.
*Alert severity	From the drop-down menu, select a severity for the alert from one of the following options: • Critical • Fatal • Major • Minor • Notification
*Event type	From the drop-down menu, select the event type that will trigger the alert: • SSH key expiry alert • Compliance alert • SSH key push failure alert • SSH discovery failure alert • SSH key deletion alert • SSH host modify/delete alert

Field	Description
*Expires in (days)	 Note: This field is applicable only for the SSHkey expiry alert. From the drop-down menu, select the number of days until the SSH key expires. The AppViewX system will trigger an alert message when this value is reached.
*SSH keygroup	 Note: This field is applicable only for the Compliance alerts, SSHkey push failure alert, and SSH key deletion alert From the drop-down menu, select the key group to be used as the basis for the alert.
*Key alert criterion	 Note: This field is applicable only for the SSH key push failure alert and the SSH key deletion alert. Select the keys you want to include in the alert, from the following options: • Logged in user keys • All user keys
*SSH host group	 Note: This field is applicable only for the SSH host modify/delete alert only. Enter the host group you want to use as the basis for the alert.
Email configuration	To send the syslog alert as an email, select this check box.
Email address	To send the syslog alert as an email, enter the email address to which this specific syslog alert will be sent.  Note: Separate multiple email addresses with a comma.
Subject	To send the syslog alert as an email, enter a subject line.
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
*Destination IP	Enter the destination IP address for the alert.

Field	Description
*Version	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2
*Port	Enter the port number to be used for the alert.
*Community string	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.
All * marked fields are mandatory.	

6. To save the SSH alerts configuration details, click **Add**.

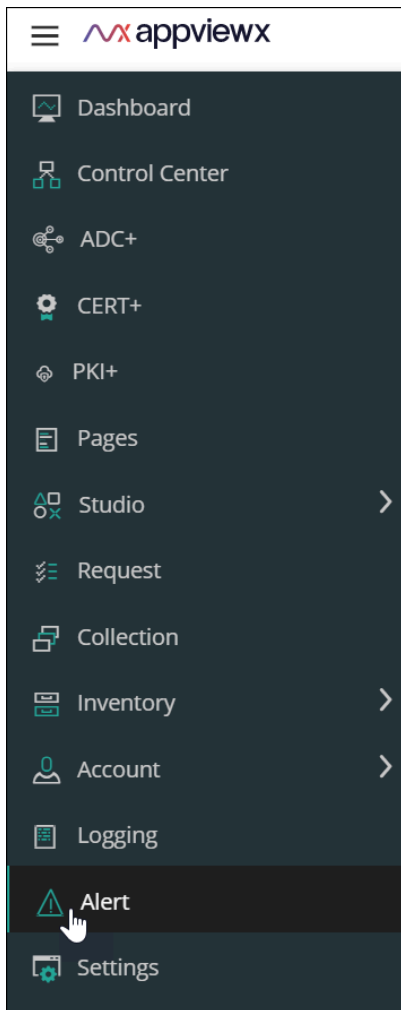
The saved details are displayed in the table shown at the bottom of the screen.

Configuring Syslog Alerts

AppViewX subscribes to all device-level alerts, where it acts as a syslog listener. Logs of any device added in AppViewX can be viewed as syslogs. However, devices tend to generate a huge amount of data. To resolve this, a Syslog Alert is a convenient way to notify about specific syslog information that is of importance to you.

To configure syslog alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

Alert :: All

1 to 100 of 6,676

All Certificate SSH ADC AppViewX Syslog

Search...

Alert detail

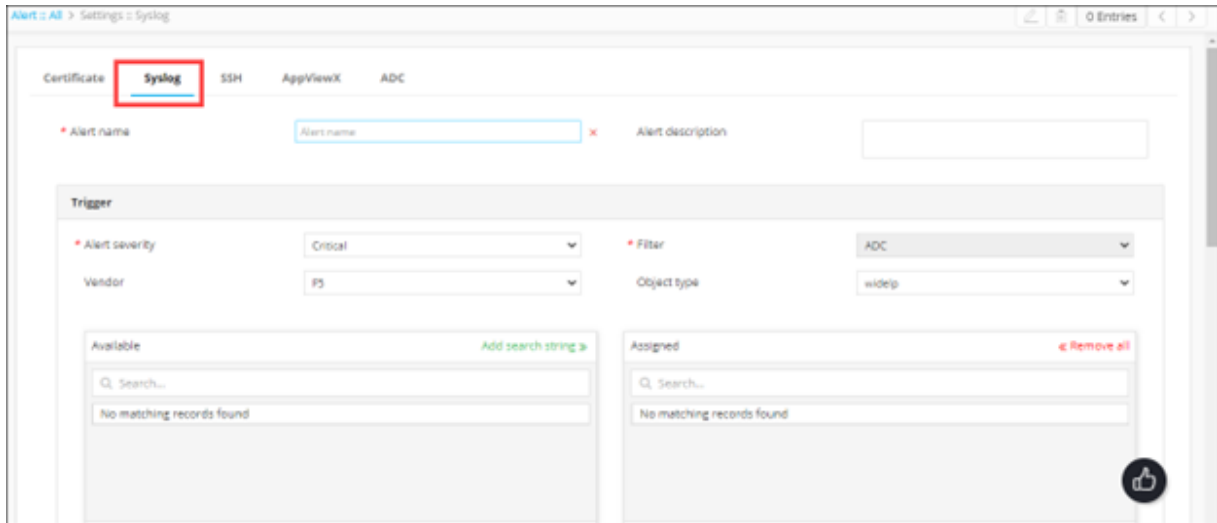
Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
03/19/2021 01:...	Alert_005658	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005657	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005656	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005655	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005654	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005653	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005652	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005651	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005650	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005649	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005648	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005647	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005646	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005645	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005644	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005643	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005642	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005641	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...
03/19/2021 01:...	Alert_005640	Failed to validate revoca...	▲ Critical	Certificate	NA	NA	NA	Revocation check Failure : The...

3. From the top-right corner of the screen, click the  icon.

The **Settings :: Certificate** page is displayed.

4. To configure Syslog alerts, click **Syslog**.

The **Settings :: Syslog** page is displayed.



5. Enter the following details:

Field	Description
*Alert name	Enter the name you want to give this alert.
Alert description	Enter a description for the alert.
All * marked fields are mandatory.	

6. In the **Trigger** section, enter the following details:

Table 1.

Field	Description
*Alert severity	From the drop-down, from the options given below, select a severity for the alert: • Critical • Fatal • Major • Minor • Notification

Field	Description
Filter	For syslog alerts, the filter is set to ADC, because syslog alerts are parsed only through ADC devices.
Vendor	ADC module vendor (A10 , Citrix , or F5)
Object type	Object type for ADC (FQDN , Service IP , VirtualService , ServiceGroup , Server , VirtualServer , or Device)
Available	Depending on the Object type and Vendor selected, a list of all available ADC objects or devices is displayed here.
Add search string	Instead of adding devices manually, AppViewX lets you automatically assign all existing devices or objects that match your criteria. To do this: - In the Available section, in the Search field, enter the search criteria. - Click Add search string.  Note: The benefit of using a search string rather than selecting devices manually is that the search string continues to work in the background and auto-assigns all new devices that match the search criteria.
Assigned	To add an object to the Assigned column, click the check box corresponding to that object.
Regex	Enter single/multiple regex patterns/strings.  Note: When entering multiple regex patterns/strings, separate the regex strings using commas. The comma works as the BOOLEAN AND operator.
All * marked fields are mandatory.	

7. In the **Action** section, enter the following details:

Field	Description
Execute workflow	To select the workflow to trigger: - Select the Execute workflow check box. - From the drop-down menu, select the workflow to trigger.

Field	Description
Metadata	AppViewX lets you define a metadata condition based on which the workflow will be triggered. To define a metadata key-value pair for this condition: - In the Enter key field, enter the key. - In the Enter value field, enter the key value. To add another key-value pair: - Click . - In the Enter key field, enter the key. - In the Enter value field, enter the key value. To delete a key-value pair: For the key-value pair you want to delete, click .

8. To send the Syslog alert as an email, execute the steps for configuring SMTP for email alerting.

9. Enter the following details:

Field	Description
Email configuration	To send the syslog alert as an email, select this check box.
Email configuration	To send the syslog alert as an email, enter the email address to which this specific syslog alert will be sent.  Note: Separate multiple email addresses with a comma.
Email configuration	To send the syslog alert as an email, enter a subject line.
All * marked fields are mandatory.	

10. To use the Simple Network Management Protocol (SNMP) to send the alert, enter the following details:

Field	Description
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
*Destination IP	Enter the destination IP address for the alert.

Field	Description
*Version	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2
*Port	Enter the port number to be used for the alert.
*Community string	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.
All * marked fields are mandatory.	

11. To save the Syslog alerts configuration details, click **Add**.

The saved details are displayed in the table shown at the bottom of the screen.

Editing Alerts

To edit an alert:

1. Navigate to the Settings page for the alert you want to edit (certificate, syslog, SSH, AppViewX, or ADC).
2. Scroll to the bottom of the page for the table that records all the alerts that have been configured for that category.
3. From the table, to select the alert you want to edit, select the check box corresponding to that alert.
4. From the top-right corner of the screen, click .
5. The fields are populated with the details of the alert.
6. Update the required fields and click **Update**.

Deleting Alerts

To delete an alert:

1. Navigate to the Settings page for the alert you want to delete (certificate, syslog, SSH, AppViewX, or ADC).
2. Scroll to the bottom of the page for the table that records all the alerts that have been configured for that category.
3. From the table, to select the alert you want to delete, select the check box corresponding to that alert.
4. From the top-right corner of the screen, click .
5. In the **Confirmation** dialog box, click **Yes**.

Searching for Alerts

AppViewX lets you search for alerts in two ways:

- Based on a timestamp
- Based on the values recorded for each alert
- [Based on a Timestamp](#)
- [Based on the Values Recorded for each Alert](#)

Based on a Timestamp

To search for alerts based on a timestamp:

1. From the **Search** field on the **Alert** page, click .
- Widgets to select the date and time are displayed.

The screenshot shows a 'Managing Alerts' dialog box with two main sections for date and time selection, labeled 'From' and 'To'.

From Section:

- Date:** A calendar for March 2021. The date 16 is highlighted in yellow.
- Time:** Set to 12:00:00 AM. Below this are three slider controls for Hour, Minute, and Second, each with a small square indicator.

To Section:

- Date:** A calendar for March 2021. The date 16 is highlighted in yellow.
- Time:** Set to 12:00:00 AM. Below this are three slider controls for Hour, Minute, and Second, each with a small square indicator.

At the bottom of the dialog are two buttons: 'Reset' and 'OK'.

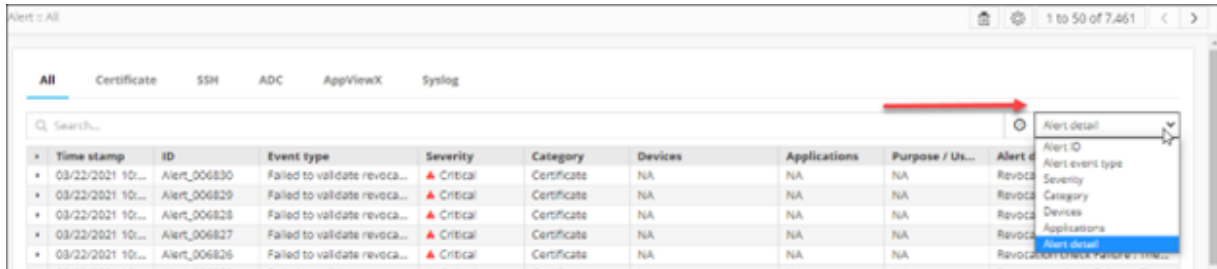
2. To select a date range, in the **From** and **To** fields, select the required dates.
3. To set a time, use the **Hour**, **Minute**, and **Second** slider controls.
4. Click **OK**.
5. The page is updated to display alerts from the selected timestamp.



Note: To view alerts from a specific date to the current date, select only the From date. When the To field is left blank, by default, it is set to the current date.

Based on the Values Recorded for each Alert

1. From the drop-down menu in the **Search** field, select the category for searching alerts. For example, to search for alerts with a specific alert ID, from the drop-down menu, select **Alert ID**.



2. In the **Search** field, enter the search value. For our example, in the Search field, enter the required alert ID.

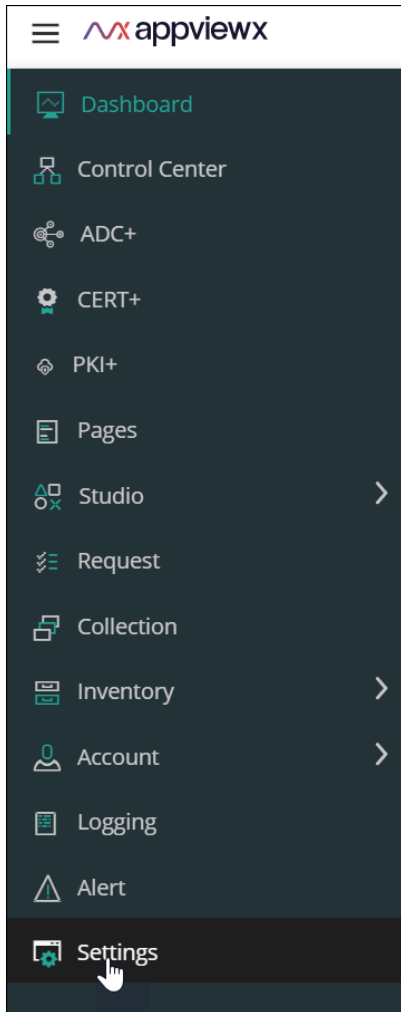
The page is updated to display alerts that fulfil the search criteria.

Purging Alerts

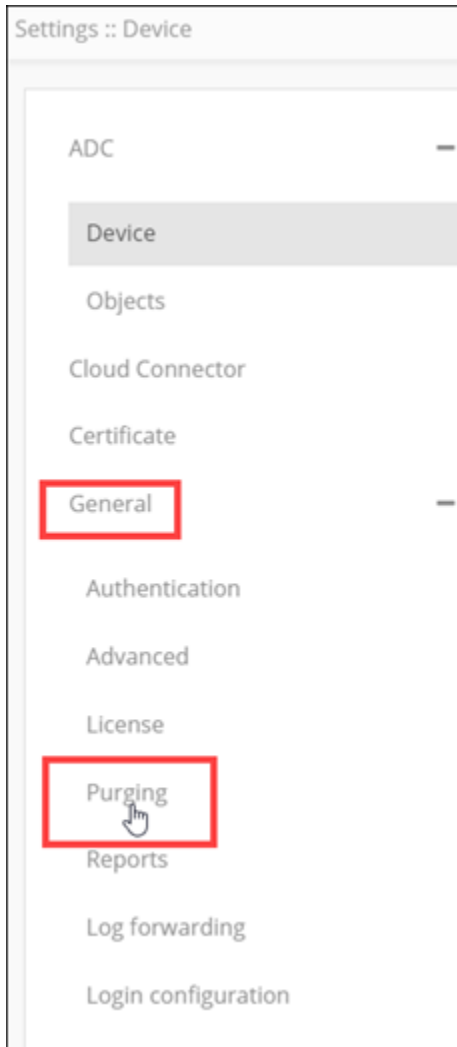
With a large number of alerts being recorded each day, a system can soon become vulnerable to threats like compromise of confidential information, a surplus of outdated information, and so on. For security reasons, regular purging of old data comes as a highly recommended practice.

To enable purging of alert records:

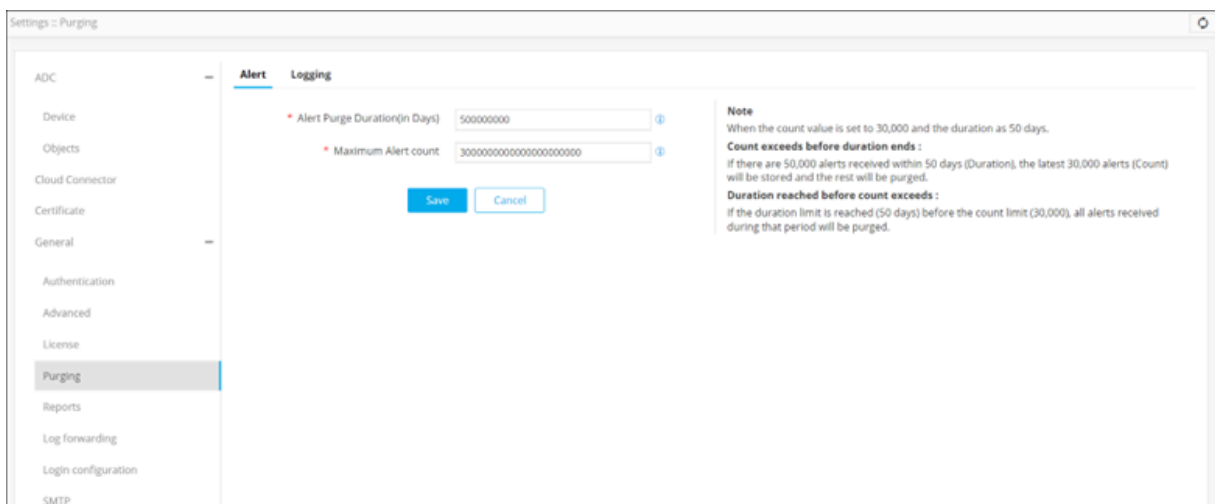
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Purging**.



The **Settings :: Purging** screen is displayed, with the **Alert** tab open by default.



5. Enter the following details:

Field	Description
*Alert Purge Duration (in Days)	Enter the number of days, the interval, after which the alerts will be purged.
*Maximum Alert count	Enter the maximum number of the most recent alerts that have to be retained. For example, if you set this value to 10,000, all alerts after the most recent 10,000 alerts will be purged.
All * marked fields are mandatory.	



Note: Excess alerts will be purged even if the maximum alert count is exceeded before the next purging cycle is scheduled.

6. Click **Save**.

Chapter 9: Managing Licenses

- [Overview](#)
- [Upgrading Licenses](#)
- [Viewing Licensing Details](#)

Overview



Note: AppViewX blocks the usage of the product if the license has expired. If an organization exceeds the threshold of license (maximum number of ADC+ objects, CERT+ certificates, and/or SECURITY+ devices allowed), a warning is issued as a reminder. A pop-up warning is issued for both scenarios.

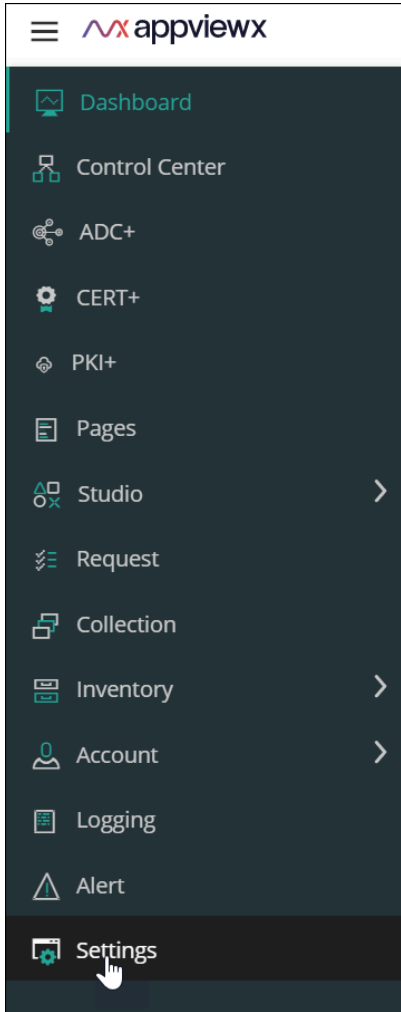
Upgrading Licenses



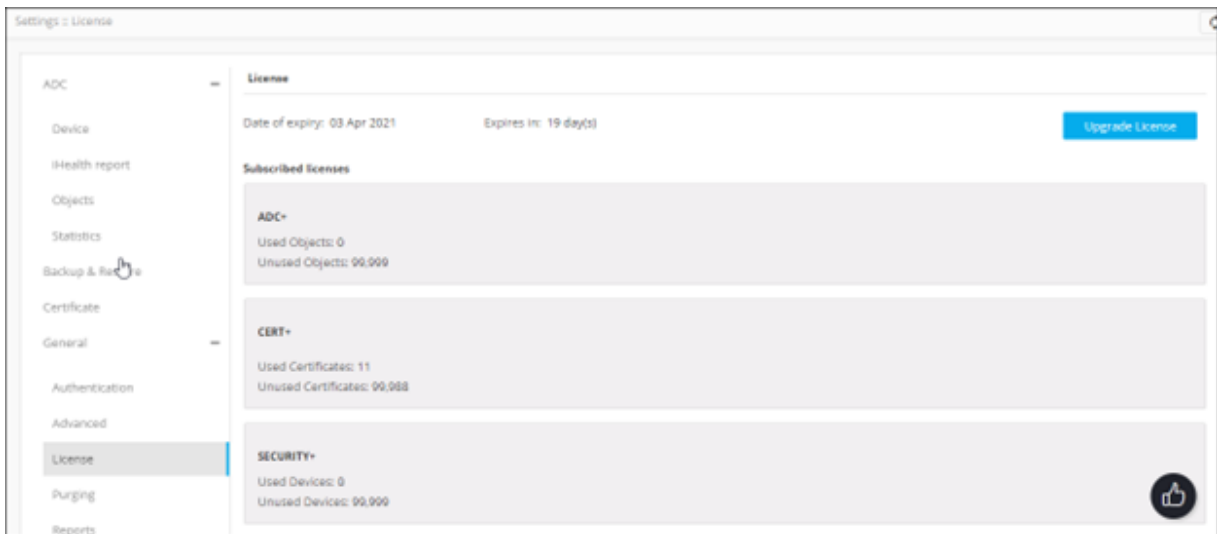
Note: AppViewX blocks the usage of the license if the license has expired. If an organization exceeds the threshold of license (maximum number of ADC+ objects, CERT+ certificates, and/or SECURITY+ devices allowed), a warning is issued as a reminder. A pop-up warning is issued for both the scenarios.

To upgrade a license:

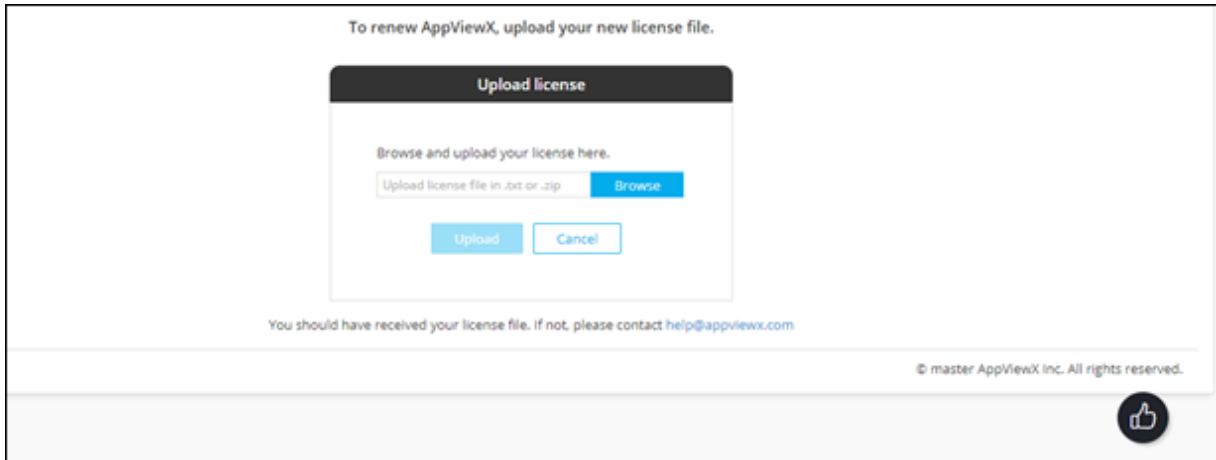
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General** and select **License**. The **Settings :: License** page is displayed.



4. To upgrade a license, from the top right corner of the screen, click **Upgrade License**.
A screen that lets you upload the license file is displayed.



5. In the **Upload License** dialog box, to upload a license file, click **Browse**.



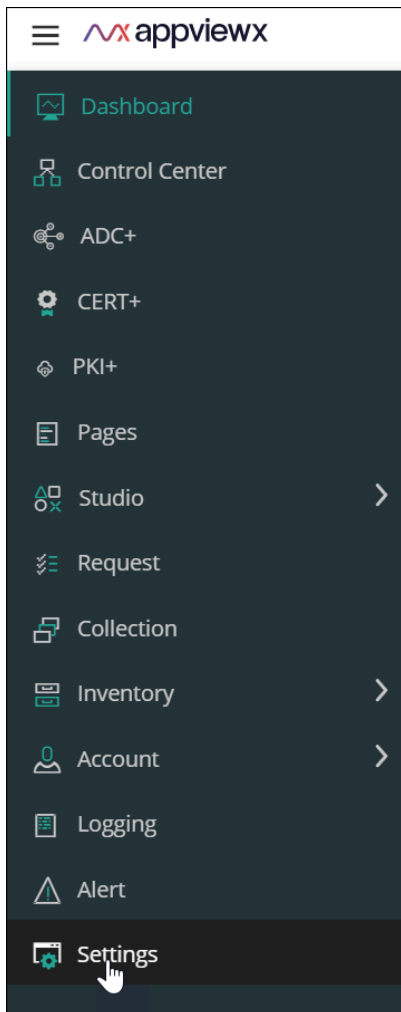
Note: License files only in the following formats can be uploaded: .txt and .zip.

6. Navigate to the location of the license file, select the file , and click **Open**.
7. Click **Upload**.

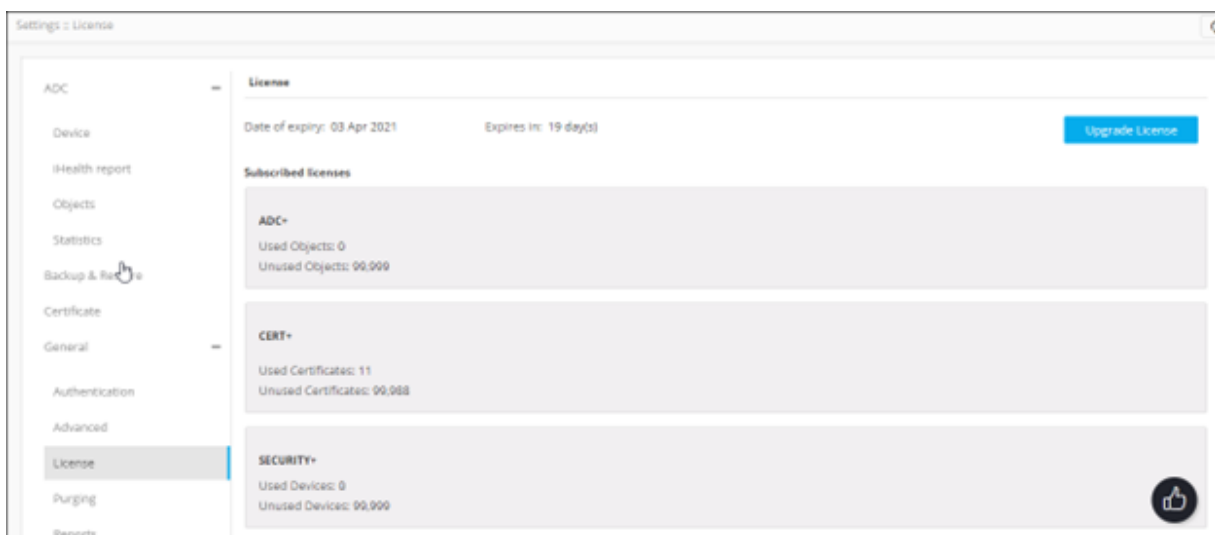
Viewing Licensing Details

To view the list and details of subscribed licenses:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General** and select **License**.
The **Settings :: License** page is displayed.



The page shows the following details:

License Detail	Description
Date of expiry	Date of expiry of the licenses
Expires in	Number of days till the license expires
Subscribed licenses	This includes the details of licenses of all AppViewX products.
Used Objects (for ADC+ licenses)	Each ADC+ license subscription allows the user a fixed number of objects that they can use. This is the number of ADC+ objects currently in use.
Unused Objects (For ADC+ licenses)	Each ADC+ license subscription allows the user a fixed number of objects that they can use. This is the number of ADC+ objects left for use.
Used Certificates (for CERT+ licenses)	Each CERT+ license subscription allows the user a fixed number of certificates that they can manage using this license. This is the number of CERT+ certificates currently being managed by the license.
Unused Certificates (for CERT+ licenses)	Each CERT+ license subscription allows the user a fixed number of certificates that they can manage using this license. This is the number of CERT+ certificates left.
Used Devices (for SECURITY+ licenses)	Each SECURITY+ license subscription allows the user a fixed number of devices that will be covered under that subscription. This is the number of devices currently in use.
Unused Devices (for SECURITY+ licenses)	Each SECURITY+ license subscription allows the user a fixed number of devices that will be covered under that subscription. This is the number of devices left for use.

Chapter 10: Customizing the AppViewX User Interface

- [Overview](#)
- [Customizing the Email Attachment Representation](#)
- [Customizing the Login Screen](#)
- [Customizing the Logo](#)
- [Customizing the Screen Header](#)

Overview

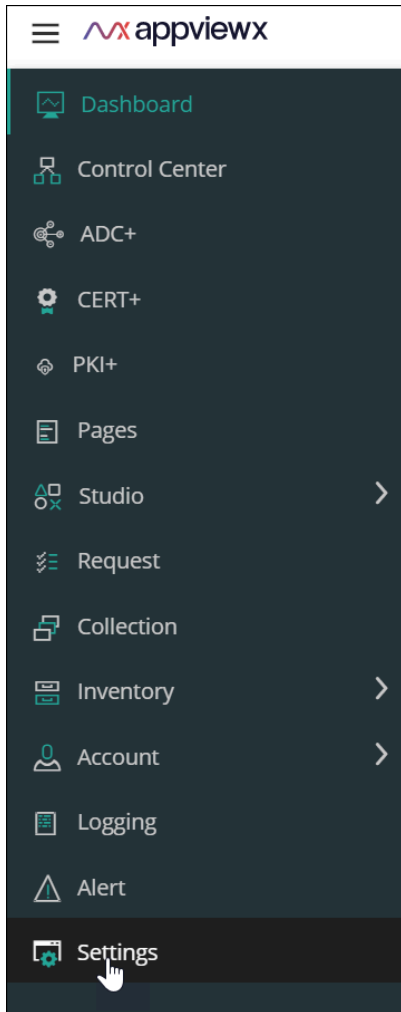
AppViewX lets you create a custom theme by customizing the following UI elements:

- Logo
- Screenheader
- Login screen
- Email attachment representation

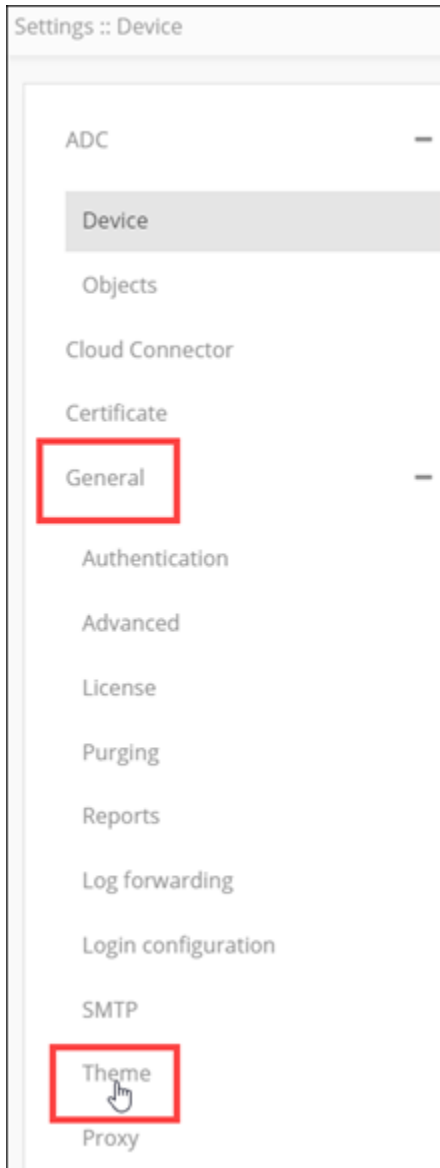
Customizing the Email Attachment Representation

To customize the cosmetics of how email attachments are represented:

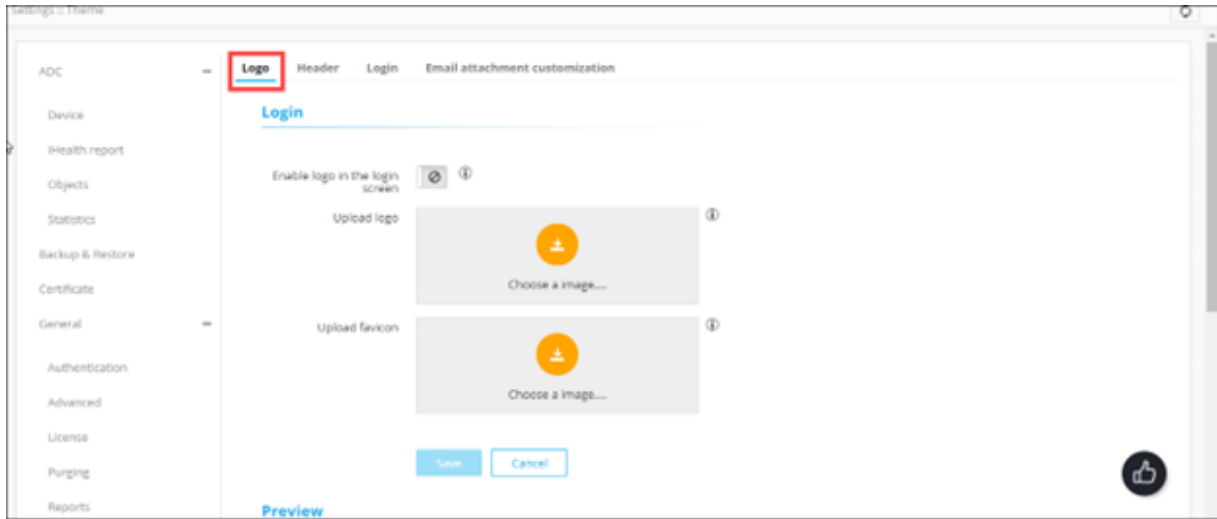
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



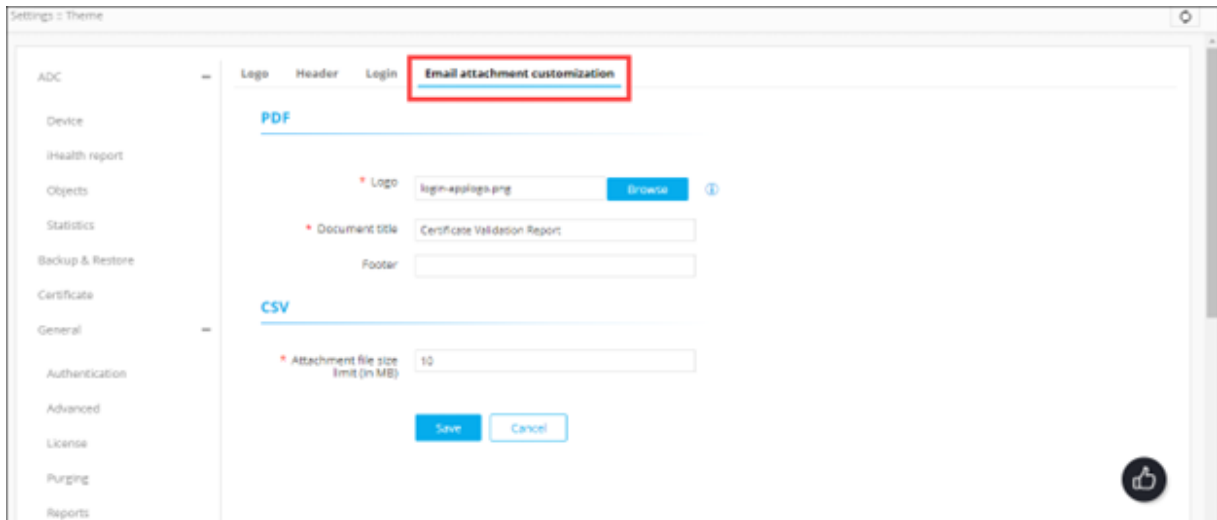
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Theme**.



The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. Click the **Email attachment customization** tab.



6. In the PDF section, enter the following details:

Field	Description
*Logo	To upload a logo image for the attachment: - Click Browse. - Navigate to the location of the image, select the image, and click Open.  Note: The image size must be less than 5 MB.
*Document title	Name to be assigned to the PDF when is it is downloaded.
Footer	Footer content to be added to the PDF.

7. In the **CSV** section, enter the **Attachment file size limit (in MB)**.



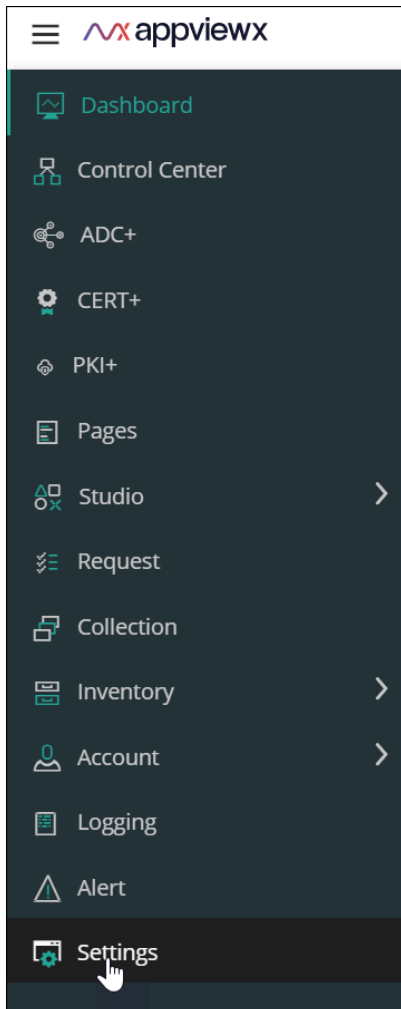
Note: This is a mandatory field.

8. To apply the changes configured above, click **Save**.

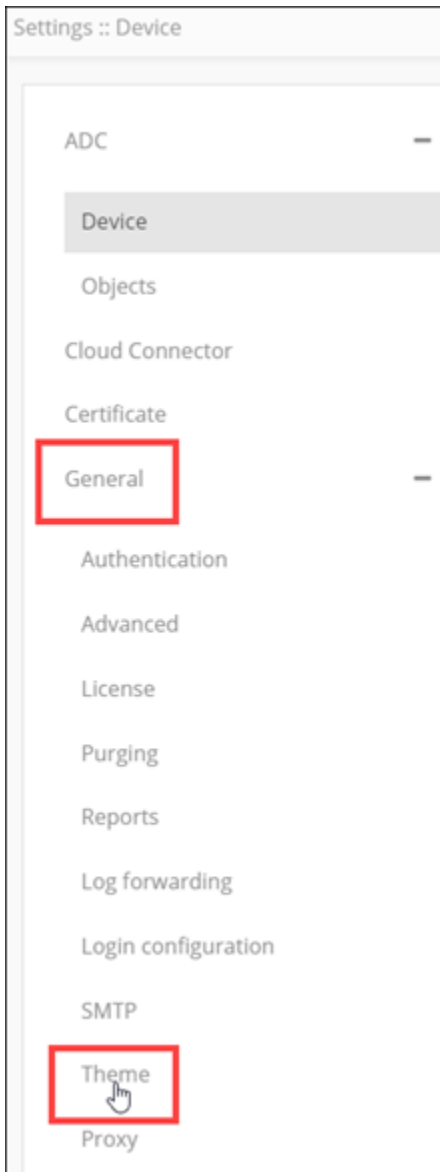
Customizing the Login Screen

To customize the login screen:

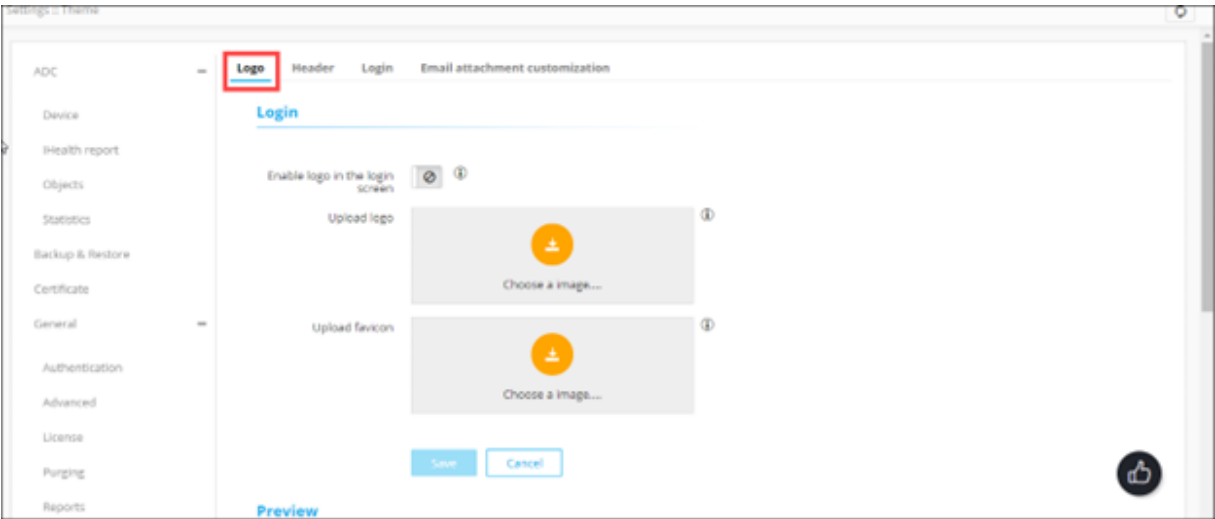
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



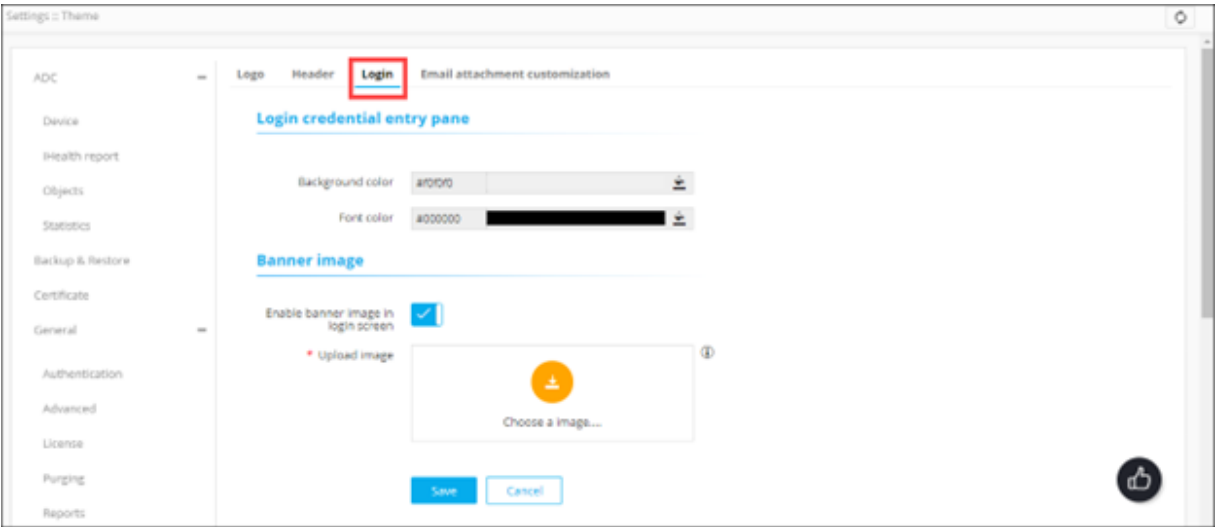
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Theme**.



The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. To customize the login screen, click the **Login** tab.



6. In the **Login credential entry pane** section, enter the following details:

Field	Description
Background color	To set a background color for the login screen: a. Enter the hex code of the required background color. OR b. To select a color, click  .
Font color	To set a font color for the text on the login screen:

Field	Description
	a. Enter the hex code of the required font color. OR b. To select a color, click .

7. In the **Banner image** section, enter the following details:

Field	Description
Enable banner image in login screen	To display a banner image on the login screen, turn on this toggle.
Upload image*	 Note: This field is enabled only when the Enable banner image in login screen is turned on. To upload a banner image: a. Click . b. From Windows Explorer, navigate to the location of the image, select the image, and click Open.  Note: - Image formats allowed for upload: .jpg, .jpeg, and .png - Recommended image resolution: 500 X 500 (width X height) - Image size: < 5 MB c. In the Confirmation Message dialog box, click Yes.

8. In the **Preview** section, view a preview of your customization for the login screen.

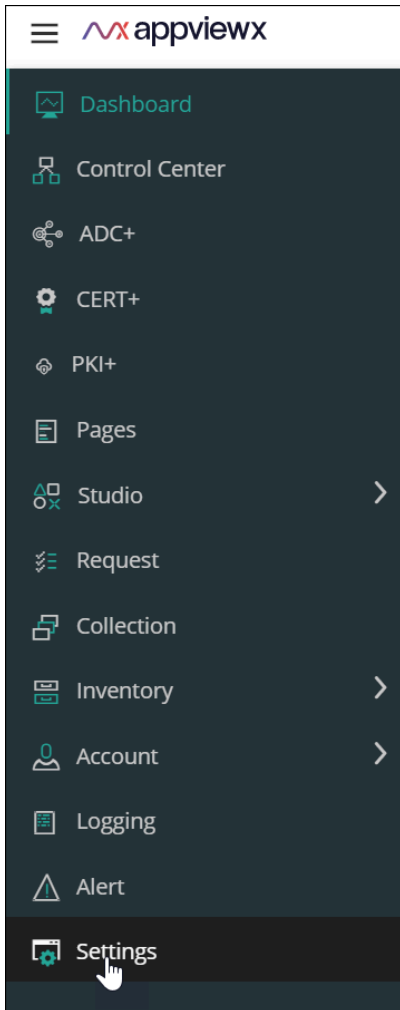
9. To apply the changes, click **Save**.

Customizing the Logo

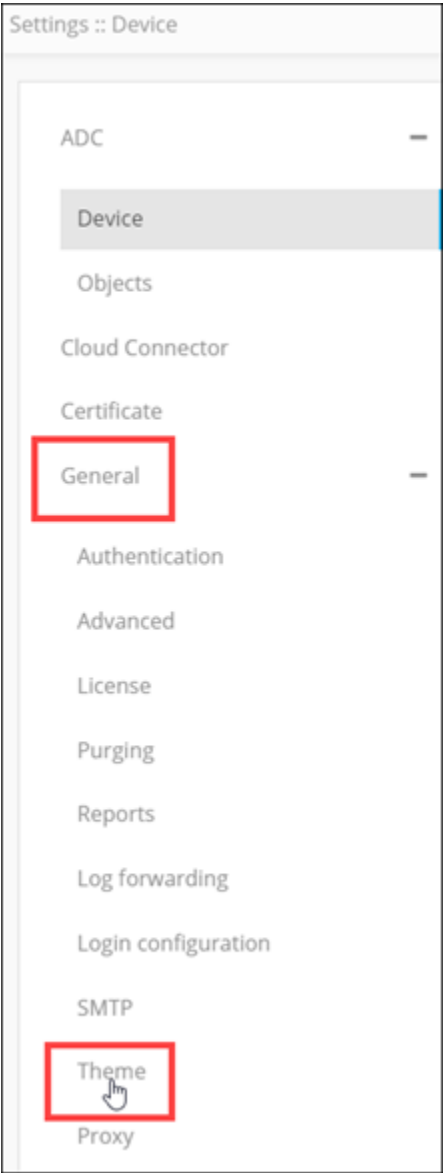
You can replace the AppViewX logo with the logo of your organization.

To add a custom logo:

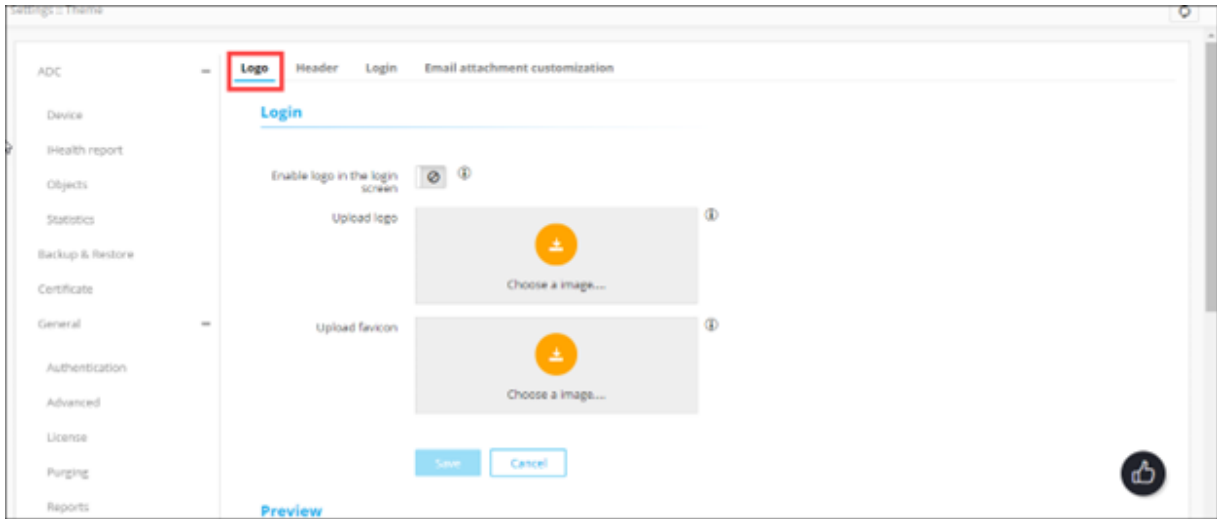
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Theme**.



The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. In the **Login** section, enter the following details:

Field	Description
Enable logo in the login screen	To display your organization's logo on the AppViewX screen, turn on this toggle.  Note: If this toggle key is disabled, AppViewX's default theme settings are applied.
Upload logo	 Note: This field is enabled only when the Enable logo in the toggle screen toggle is turned on. To choose a logo image: - Click . - From Windows Explorer, navigate to the location of the logo image, select the image, and click Open.  Note: - Image formats allowed for upload: .png and .svg - Maximum image resolution allowed: 865 X 185 (width X height)

Field	Description
	 • Image size: < 5 MB • Recommended image dimensions: 175 X 37 (width X height) c. In the Confirmation Message dialog box, click Yes.
Upload favicon	 Note: This field is enabled only when the Enable logo in the toggle screen toggle is turned on. To choose a favicon image: a. Click . b. From Windows Explorer, navigate to the location of the logo image, select the image, and click Open.  Note: • Image formats allowed for upload: .png • Maximum image resolution allowed: 64 X 64 (width X height)Ima • Image size: < 5MB c. In the Confirmation Message dialog box, click Yes.

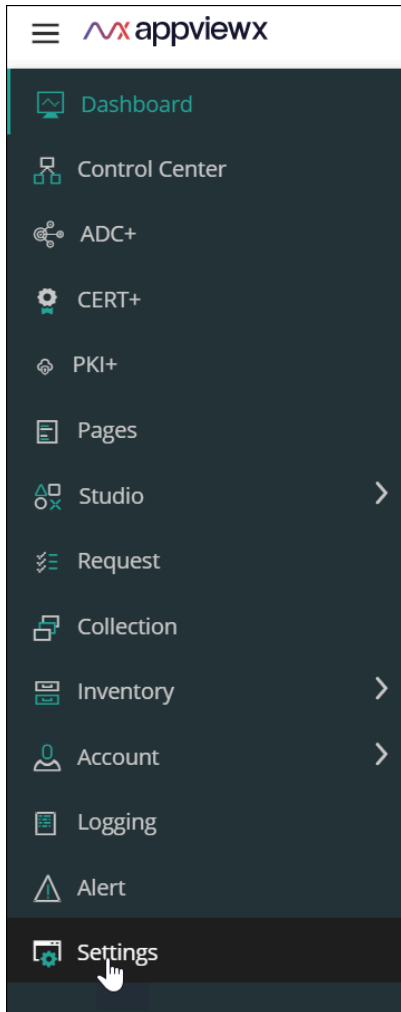
6. In the **Preview** section, view a preview of the login screen after your custom logo and favicon have been uploaded.

7. To apply the changes, click **Save**.

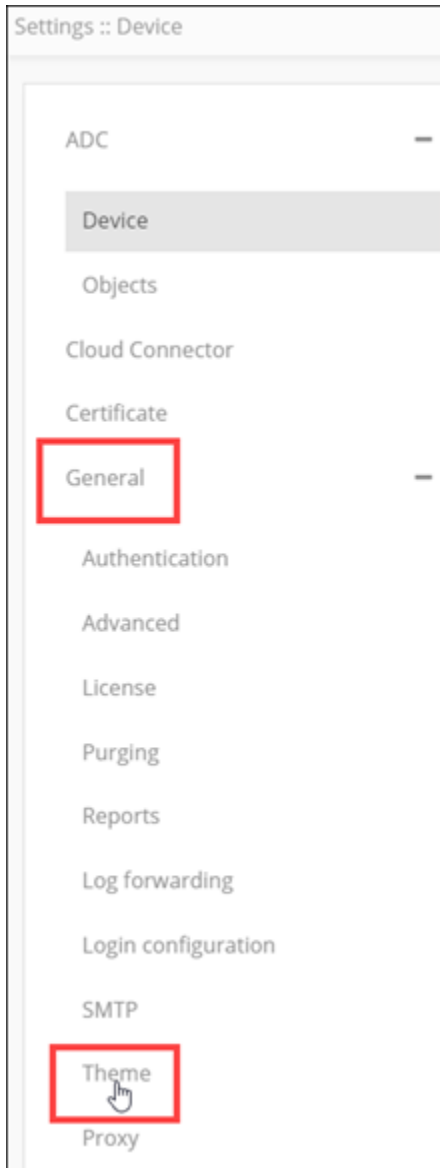
Customizing the Screen Header

To customize the screen header:

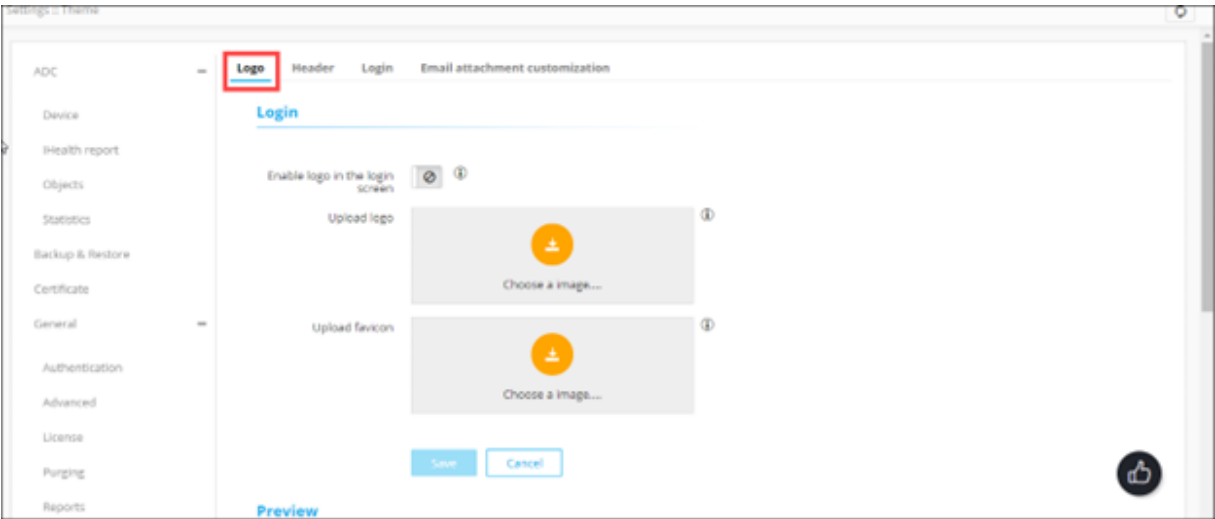
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



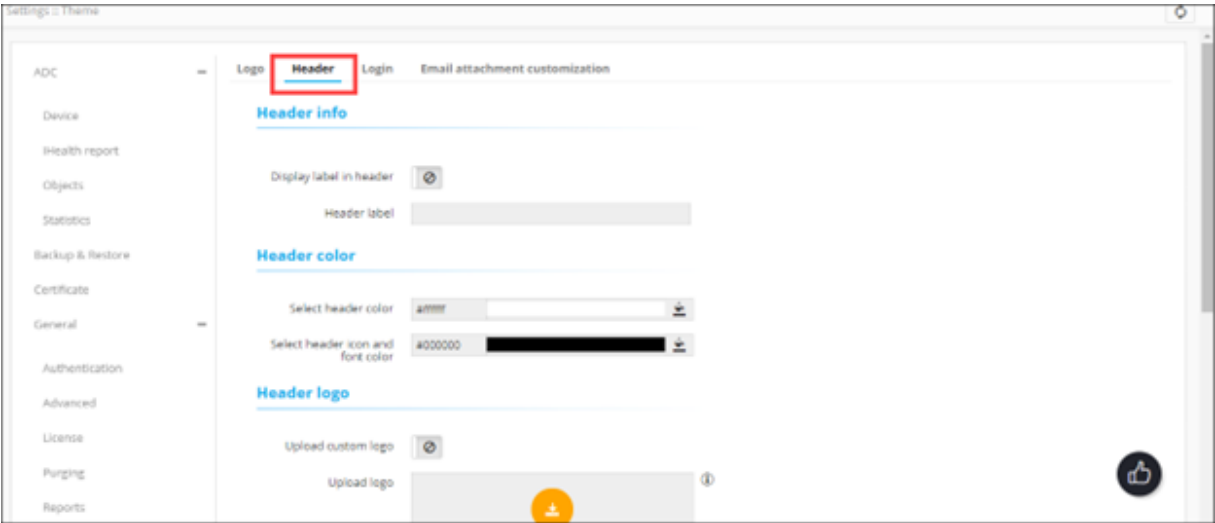
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Theme**.



The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. To customize the screen header, click the **Header** tab.



6. In the **Header Info** section, enter the following details:

Field	Description
Display label in header	To display custom header text, turn on this toggle.
Header label	Enter the custom header text.  Note: This field is enabled only when the Display label in header toggle is turned on.

7. In the **Header color** section, enter the following details:

Field	Description
Select header color	To set a color for the header text: • Enter the hex code of the required header color. OR • To select a color, click .
Select header icon and font color	To set a color for the header icon and the font: • Enter the hex code of the required color. OR • To select a color, click .

8. In the **Header logo** section, enter the following details:

Field	Description
Upload custom logo	To insert a custom logo image in the header, turn on this toggle.
Upload logo	 Note: This field is enabled only when the Upload custom logo toggle is turned on. To upload a logo image: a. Click . b. From Windows Explorer, navigate to the location of the image, select the image, and click Open.  Note: • Image formats allowed for upload: .png and .svg • Maximum image resolution allowed: 865 X 185 (width X height) • Image size: < 5 MB • Recommended image dimensions: 175 X 37 (width X height) c. In the Confirmation Message dialog box, click Yes.

9. In the **Preview** section, view a preview of your header customization.
10. To apply the changes, click **Save**.

Chapter 11: Glossary

Term	Definition
HSM	An HSM (Hardware Security Module) is a piece of hardware and associated software or firmware that usually resides in a PC or server and provides at least the minimal cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing.
LDAP	The Lightweight Directory Access Protocol (LDAP) is an authentication protocol to validate a user's credentials, entered in an application, against the credentials stored in the Active Directory database.
PAM	Privileged Access Management (PAM) is the practice of managing users/devices/applications that have elevated access to an organization's most confidential and critical resources.
RADIUS	The Remote Authentication Dial-In User Service (RADIUS) protocol is a networking protocol that provides centralized authentication, authorization, and accounting management.
RBAC	Role and Resource-Based Access Control (RBAC) is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise.
Resource	All the devices and objects that are configured within AppViewX are termed as Resources. Resources can be assigned to a user group. Users within a user group will inherit resources assigned to that group. User groups can be assigned more than a resource.
Role	A set of permissions to execute specific tasks in the application is termed as Roles in AppViewX. Roles can be assigned only to a user group. Users within user groups will inherit role permissions assigned to that group. User groups can be assigned more than one role.
SAML	The SecurityAssertion Markup Language (SAML) protocol is used for authenticating and authorizing user identity for Single Sign On (SSO) services.
TACAS	The Terminal Access Controller Access Control System (TACACS) authentication is used to validate users requesting remote access.

Term	Definition
User	A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directories (AD).
User Group	user group is a set of individual users assigned with the same roles and resources. You can associate one or more roles and resources to a user group. Users within that user group are granted the role and resource permissions.