Access Manager Passwordless Authentication

April 2024

Passwordless authentication differs from traditional username and password-based login systems. Instead of requiring users to remember and input a password, it uses biometrics, one-time codes sent via SMS or email, or a physical security key.

Why passwordless authentication

Passwordless authentication provides several benefits, including:

- Improved security: Eliminates the risk of weak or stolen passwords, thereby reducing the risk of account takeovers and data breaches.
- Increased convenience: Eliminates the need to remember complex passwords, thereby reduces the risk of forgotten passwords and locked accounts.
- Faster logins: Allows users to log in almost instantly through passwordless authentication methods, such as biometrics or security keys.
- Lightning-fast workstation logins: Allows employees to log in to their workstations more quickly, increases productivity, closes security gaps, and reduces frustration.
- Reduced helpdesk calls: Eliminates the need to remember or reset any passwords. The helpdesk team can focus on other crucial tasks.
- Secure Payments with Reduced Friction: In addition to making the transaction more secure, it reduces friction in the check out process, leading to higher conversion rates and better customer satisfaction.
- Better compliance with regulations: Assists companies in meeting regulatory compliance requirements, such as the General Data Protection Regulation (GDPR).

How Access Manager supports passwordless authentication

You can configure passwordless authentication in Access Manager by using one of the following features:

- **Kerberos Authentication**: For information, see Kerberos Authentication in the NetIQ Access Manager 24.2 (v5.1) Administration Guide.
- **Certificate-based Authentication**: For information, see Mutual SSL (X.509) Authentication in the NetIQ Access Manager 24.2 (v5.1) Administration Guide.

- **Integration with NetIQ Advanced Authentication**: When integrated with NetIQ Advanced Authentication, Access Manager supports passwordless authentication through one of the following Advanced Authentication methods:
    - FIDO2
    - FIDO U2F
    - Bluetooth
    - Smartphone
    - Facial Recognition
    - Fingerprint
    - Card (NFC)
    - PKI

NOTE: The plug-in-based integration does not support Bluetooth and Facial Recognition methods.

ⓘ This guide includes details and instructions for passwordless authentication using the *FIDO2* method of Advanced Authentication.

In this Article

- A Sample Scenario for Passwordless Authentication
- Prerequisites for Configuring Passwordless Authentication Using Advanced Authentication
- Enabling Passwordless Authentication Using Advanced Authentication

1 A Sample Scenario for Passwordless Authentication

ABC bank wants to provide customers with secure and convenient access to their online accounts. The bank does not want customers to remember and input a complex password each time they log in to their banking accounts. In addition, it wants to prevent the risk of intercepted credentials.

In this scenario, the bank implements the FIDO2-based Passwordless authentication feature of NetIQ Access Manager. Passwordless authentication improves the user experience, increases security, and reduces the risk of account takeovers.

Maria is a customer of the bank. She wants to check her account balance and transaction history on her cell phone. She has a FIDO2 security key. She performs the following actions:

1. Opens the ABC mobile banking app.
2. Clicks the **Log in with security key**.

   The system prompts her to insert her security key into USB-C port or NFC reader.
3. Inserts the key and touches the button to confirm her identity.

   The system verifies her identity and grants her access to her account without requiring a password.

2 Prerequisites for Configuring Passwordless Authentication Using Advanced Authentication

❐ Access Manager is installed and configured.

See *NetIQ Access Manager CE 24.2 (v5.1) Installation and Upgrade Guide*.

❐ Advanced Authentication or Advanced Authentication as a Service is installed and configured.

For information about how to install Advanced Authentication, see Advanced Authentication Server Installation and Upgrade Guide.

For information about how to configure Advanced Authentication or Advanced Authentication as a Service, see Advanced Authentication Administration Guide.

❐ An Access Manager administrator account is available.

❐ An Advanced Authentication administrator account is available.

3 Enabling Passwordless Authentication Using Advanced Authentication

Enabling passwordless authentication consists of the following tasks:

1. Integrating Advanced Authentication with Access Manager
2. Configuring Passwordless Authentication
3. Verifying the Integration
4. End-Users Enrollment in the Advanced Authentication Self-Service Portal

3.1 Integrating Advanced Authentication with Access Manager

You can integrate Advanced Authentication with Access Manager by using any one of the following approaches:

- Plug-in-based approach
- OAuth-based approach (Recommended)

For more information about these approaches and their differences, see Implementation Approaches.

To integrate both products, you must first configure the Advanced Authentication server and then configure the Advanced Authentication server details in Access Manager.

- Configure the Advanced Authentication Server
- Configure the Advanced Authentication Server Details in Access Manager

3.1.1 Configure the Advanced Authentication Server

1 Log in to Advanced Authentication as an administrator.

2 Verify that the `NAM` event is available in **Events**.

NOTE: The NAM event is created by default when you install Advanced Authentication. In a rare scenario, the NAM event is not created by default. Re-installing Advanced Authentication resolves the issue.

3 Set up a central user store that both Advanced Authentication and Access Manager will use while authenticating a user. You can add a new repository in the Advanced Authentication server or configure details of an existing Access Manager user store.

If you add a new repository in Advanced Authentication, configure the same repository when you Configure the Advanced Authentication Server Details in Access Manager.

For more information about how to add a repository, see Adding a Repository.

4 Configure a method that supports passwordless authentication. For example, configure FIDO2.

An Advanced Authentication method verifies the identity of a user who tries to access resources.

For more information about how to configure a method, see Configuring Methods.

5 Create a chain.

A chain is a combination of methods. A user must execute and succeed all methods in a chain to be authenticated. Add the FIDO2 method that you configured in the previous step. In **Roles and Groups**, assign the chain to the user group configured in the repository.

For example, specify *XYZ*`\Allowed RODC Password Replication Group`, where *XYZ* is the repository name.

For more information about configuring chains, see Creating a Chain.

6 (Required only for the OAuth-based approach) Configure an event.

IMPORTANT: In the plug-in-based integration, Access Manager uses the default NAM event created during Advanced Authentication installation.

Perform the following steps to configure an event:

6a Click **Events** > **Add**.

6b Specify a name for the event.

6c Select **OAuth2** from **Event type**.

6d Select the chain you created in the previous step.

NOTE: You need the Client ID and Client secret while configuring the Advanced Authentication server in Access Manager. You cannot view the Client secret later, so you must note the value.

6e In **Redirect URIs**, specify `https://`*`<identity server-url>`*`:`*`<port>`*`/nidp/oauth/nam/callback`.

For example, if the Identity Server URL is `https://domain.example.com:8443/nidp`, where `domain.example.com` is the domain name, and 8443 is the port, specify `https://domain.example.com:8443/nidp/oauth/nam/callback`.

IMPORTANT: If your Identity Server base URL is on the standard SSL port 443, do not include the port number in the URI. For example, `https://domain.example.com/nidp/oauth/nam/callback`.

7 (Required only for the Plug-in-based approach) Assign the created chain to the NAM event in the Advanced Authentication server.

8 Continue with "Configure the Advanced Authentication Server Details in Access Manager" on page 5.

3.1.2 Configure the Advanced Authentication Server Details in Access Manager

Before integrating Access Manager with Advanced Authentication or Advanced Authentication as a Service, log in to the Identity Server machine, go to `/opt/novell/nam/idp/plugins/aa/`, and ensure that the `config.xml` file does not exist in this location. Perform this check on all Identity Server nodes.

1 On the **Home** page, click **Identity Servers > IDP Global Settings** > **Advanced Authentication**.

2 Specify the following details:

Field	Description
Server Domain	Specify the scheme, domain name, and port of the Advanced Authentication server.
Tenant Name	Specify the name of the tenant that you want to use. This field populates the TOP tenant of Advanced Authentication by default. You can specify another tenant name that you want to use.

NOTE: When using the Plug-in-based methods, skip to Step 5 on page 6.

3 (Required only for OAuth-based approach) Select **Integrate using OAuth** under **OAuth Event Configuration**.

4 (Required only for OAuth-based approach) Specify the following details:

Field	Description
Event Name	Specify an event name. This event name must be identical to the event name specified in the Advanced Authentication administration portal.
Client ID	Specify the client ID generated while creating the OAuth 2.0 event in the Advanced Authentication administration portal.
Client Secret	Specify the client secret generated while creating the OAuth 2.0 event in the Advanced Authentication administration portal.

Access Manager uses the endpoint links to retrieve token and user details from the Advanced Authentication server. These are default endpoint links. If the values of the URIs change because of modification of the Advanced Authentication authorization server, then you can change the same here.

Field	Description
Authorization URL	Access Manager uses this URL to retrieve the authorization code from the Advanced Authentication server.
Token URL	Access Manager uses this URL to exchange the authorization code with the access token.
User Info URL	Access Manager sends the access token to this URL to get the user details from the Advanced Authentication server.

The fields under Integration URLs are auto-populated after you specify the server domain address.

Field	Description
Enrollment Page URL	If the user is not enrolled in the Advanced Authentication server, then Access Manager uses this URL to redirect the user to the enrollment page.
Sign Data URL	Access Manager uses this URL to retrieve the signed data from the Advanced Authentication server.

5 Click **Save**.

6 Log in to the Identity Server machine, go to `/opt/novell/nam/idp/plugins/aa/`, and verify that the `config.xml` file is available in this location. Perform this check on all Identity Server nodes.

7 Verify that the endpoint has been created in the Advanced Authentication server.

Go to the Advanced Authentication administration portal and verify that the hostname or domain name of the Identity Server Cluster is displayed as the endpoint under **Endpoints**.

8 On the **Home** page, click **Certificates** > **Trusted Roots** to verify if the Advanced Authentication server certificate is available.

If the certificate is not available, then perform the following steps to import the certificate:

8a Click **Certificates** > **Trusted Roots** > **Auto-Import From Server**.

8b Specify the server IP/DNS, server port, and certificate name.

8c Click **OK**.

9 Configure the same user store or repository added in the Advanced Authentication server. See Step 3 on page 4.

9a On the **Home** page, click **Identity Servers** > *[cluster name]* > **User Stores** > Plus icon.

9b Specify the details and click **Finish**.

9c Update Identity Server Cluster.

Skip this step if you have configured an existing Access Manager user store in the Advanced Authentication server.

10 Continue with Section 3.2, “Configuring Passwordless Authentication,” on page 6.

3.2 Configuring Passwordless Authentication

Configure Advanced Authentication to perform the first-factor authentication.

- Configuring Passwordless Authentication using the OAuth-based Approach
- Configuring Passwordless Authentication using the Plug-in-based Approach

3.2.1 Configuring Passwordless Authentication using the OAuth-based Approach

Perform the following steps in Access Manager:

1 Configure an Advanced Authentication Generic class.

1a On the **Home** page, click **Identity Servers** > *[cluster name]* > **Authentication** > **Classes** > `Plus` icon.

1b Under **Advanced Authentication**, select **Advanced Authentication Generic Class**.

1c Specify the following details:

Field	Description
Class Name	Specify a name for the class.
Java class path	Specify the java class path.

1d Click **Next** > **Finish**.

2 Create a method for this class.

2a On the **Home** page, click **Identity Servers** > *[cluster name]* > **Authentication** > **Methods** > `Plus` icon.

2b In **Advanced Authentication Chains**, select the chain you created for FIDO2.

NOTE: If no chain is available in **Advanced Authentication Chains**, create a chain in the Advanced Authentication server. If a chain is available in the Advanced Authentication server and unavailable in **Advanced Authentication Chains**, then assign the chain to the configured Access Manager OAuth event in the Advanced Authentication administration portal.

3 Create a contract for the method.

3a On the **Home** page, click **Identity Servers** > *[cluster name]* > **Authentication** > **Contracts** > `Plus` icon.

3b In **URI**, specify a unique path value that identifies the contract. You can use URI to identify this contract for external providers. For example, specify `/nam/AAgenericcontract` or `/mycompany/name/password/form`.

3c In **Methods**, add the Advanced Authentication method created in the preceding step.

3d Click **Save**.

3e Update Identity Server Cluster.

NOTE: For a seamless Identity Server redirection, configure a Custom Response Header and add Advanced Authentication as an allowed source. For more information, see “Configuring a Custom Response Header for an Identity Server Cluster” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide* and TID.

3.2.2 Configuring Passwordless Authentication using the Plug-in-based Approach

Perform the following steps in Access Manager:

1 Configure an Advanced Authentication class.

1a On the **Home** page, click **Identity Servers** > **Authentication** > **Classes** `Plus` icon.

1b Under **Advanced Authentication**, select **SMS Class**.

1c Specify the following details:

Field	Description
Class Name	Name of the class.
Java class path	Specify the Java class path.

1d Click **Save** >

2 Create a method for this class.

2a On the **Home** page, click **Identity Servers** > `[cluster name]` > **Authentication** > **Methods** > `Plus` icon.

2b Specify a name for this method.

2c Select **Identifies User**.

2d In Advanced Settings, click the + icon, and configure the following property:

IMPORTANT: The name and the value of the property are case-sensitive.

Field	Detail
Property Name	Auth_Type
Property Value	preAuth

For more information about creating a method, see "Configuring Authentication Methods" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

IMPORTANT: FIDO U2F does not work if enrollment and authentication are performed on different domain names. With Access Manager and Advanced Authentication, you have two domain names: one for Identity Server and another for the Advanced Authentication server.

To work around this, create proxy services for Identity Server and Advanced Authentication server under the same domain name. See Configuring a FIDO U2Fin the NetIQ Access Manager 24.2 (v5.1) Administration Guide.

3 Create a contract for the method.

3a On the **Home** page, click **Identity Servers** > *[cluster name]* > **Authentication** > **Contracts** > `Plus` icon.

3b In **URI**, specify a unique path value that identifies the contract. You can use URI to identify this contract for external providers. For example, specify `/nam/AAplugincontract` or `/mycompany/name/password/form`.

3c In **Methods**, add the Advanced Authentication method created in the preceding step.

3d Click **Save**.

3e Update Identity Server Cluster.

For more information about creating a contract, see "Configuring Authentication Contracts" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

IMPORTANT: End users must enroll the methods for passwordless authentication. See Section 3.4, "End-Users Enrollment in the Advanced Authentication Self-Service Portal," on page 10.

3.3 Verifying the Integration

To verify that the integration is successful, create a dummy user account and enroll one or more authenticators.

For information about how an end user enrolls to authenticators, see Section 3.4, "End-Users Enrollment in the Advanced Authentication Self-Service Portal," on page 10.

Use this user account to access a protected resource by executing the contract created in Access Manager.

- Verifying the Plug-in-based Integration
- Verifying the OAuth-based Integration

3.3.1 Verifying the Plug-in-based Integration

Perform the following steps in Access Manager:

1. Create an Advanced Authentication class. You can use a Dynamic class or any other class except the Generic class.
2. Create a method and include the class created in the previous step, add a repository, and add the Advanced Authentication Enrollment URL property.

   Specify the URL of the Advanced Authentication portal for authenticator enrollments.

   For example:

   URL of the portal when not protected by Access Gateway: `https://<Advanced Authentication hostname or IP address>/account`

   URL of the portal when Access Gateway protects Identity Server and Advanced Authentication: `https://<Access Gateway hostname>/account`
3. Create a contract and add the Advanced Authentication method (FIDO2) created in the previous step.
4. Using the account of the dummy user, access Identity Server or a protected resource to which this contract has been assigned and execute this contract. (`https://<identity server-url>:<port>/nidp`)

   The user must be prompted to insert the security key into the USB-C port or NFC reader and confirm the identity.

   The user authenticates if the integration is successful.

3.3.2 Verifying the OAuth-based Integration

Perform the following steps in Access Manager:

1. Create a class using the Advanced Authentication Generic class.
2. Create a method, add the class, and select the required chain in **Advanced Authentication Chains**. For example, select FIDO2.
3. Create a contract. Add the Advanced Authentication method created in the previous step.
4. Using the account of the dummy user, access Identity Server or a protected resource to which this contract has been assigned and execute this contract. (`https://`*`<identity server-url>:<port>/`*`nidp`)

   Identity Server redirects the login request to Advanced Authentication OSP for the chain execution.

   On the OSP page, select the chain you configured for FIDO2. The user must be prompted to insert the security key into the USB-C port or NFC reader and confirm the identity.

   Authentication succeeds on the OSP page, and the user is redirected to Identity Server or protected resource when integration is successful.

3.4 End-Users Enrollment in the Advanced Authentication Self-Service Portal

End-users must enroll all methods of an authentication chain.

Users must perform the following steps to enroll authenticators:

1. Access the Advanced Authentication Self-Service portal.

   URL of the portal when not protected by Access Gateway: `https://<Advanced Authentication hostname or IP address>/account`

   URL of the portal when Access Gateway protects Identity Server and Advanced Authentication: `https://<Access Gateway hostname>/account`
2. Select a method from **Add Authenticator** to enroll.

   For example, to enroll the FIDO2 method, select **FIDO2**, specify the email ID, and click **Save**.

Legal Notice

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/ (https://www.microfocus.com/en-us/).