Access Manager Passwordless Authentication

March 23

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. It enhances the user experience by making the login process faster, more convenient, and more secure. Furthermore, it lowers the risk of account takeovers and data breaches caused by weak or stolen passwords.

Why to use passwordless authentication

Passwordless authentication provides several benefits, including:

- Improved security: Passwordless authentication eliminates the risk of weak or stolen passwords, reducing the risk of account takeovers and data breaches. Increased convenience: Users are no longer required to remember complex passwords, reducing the risk of forgotten passwords and locked accounts.
- Faster login times: Passwordless authentication methods such as biometrics or security keys can allow users to log in almost instantly.
- Reduced helpdesk calls: With passwordless authentication, users are less likely to forget their passwords.
- Better compliance with regulations: Passwordless authentication can assist 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 Appliance 5.0 Administration Guide.
- **Certificate-based Authentication**: For information, see Mutual SSL (X.509) Authentication in the NetIQ Access Manager Appliance 5.0 Administration Guide.
- **Integration with NetIQ Advanced Authentication**: When Access Manager is integrated with Advanced Authentication, you can configure passwordless authentication by using one the following Advanced Authentication methods:
  - FIDO2
  - FIDO U2F

- Bluetooth
- Smartphone
- Facial Recognition
- Fingerprint
- Card (NFC)

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

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 accounts.

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. When she opens the bank's mobile app and clicks the **Log in with security key**, the system prompts her to insert her security key into her phone's USB-C port or NFC reader. She 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.

Prerequisites for Configuring Passwordless Authentication Using Advanced Authentication

- ❒ Access Manager is installed and configured.

  See *NetIQ Access Manager Appliance 5.0 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.

Enabling Passwordless Authentication Using Advanced Authentication

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

Integrating Advanced Authentication with Access Manager

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

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 might not get 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 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.

An Advanced Authentication method verifies the identity of a user who tries to access resources. Configure a method that supports passwordless authentication. For example, configure the FIDO2 method.

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 needs to execute and succeed all methods of 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 that is configured in the repository. For example, specify *XYZ*\`Allowed RODC Password Replication Group`, where *XYZ* is the name of the repository.

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

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

Advanced Authentication provides authentication events for Access Manager. An event leverages the Advanced Authentication functionalities for Access Manager. Access Manager triggers the respective authentication event when a user tries to access it.

NOTE: For Plug-in based methods, you do not need to create the OAuth 2.0 event. A default NAM event is created when you install Advanced Authentication. Access Manager uses the NAM event if you integrate using the Plug-in based approach and uses the OAuth 2.0 event when you integrate using the OAuth-based approach.

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 Client ID and Client secret while configuring the Advanced Authentication server in Access Manager. You cannot view Client secret later, therefore you must make a note of this 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.

Configure the Advanced Authentication Server Details in Access Manager

Before integrating Access Manager with Advanced Authentication or Advanced Authentication as a Service, go to `/opt/novell/nam/idp/plugins/aa/` and ensure that the `config.xml` file does not exist for any Identity Server node in this location.

1 Click **Devices** > **Identity Servers** > **Shared 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 T0P 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 5.

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 that was generated while creating the OAuth 2.0 event in the Advanced Authentication administration portal.
Client Secret	Specify the client secret that was 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 values 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 **Apply**.

6 Verify that the `config.xml` file is available in each Identity Server node in `/opt/novell/nam/idp/plugins/aa/`.

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 In Access Manager, go to Dashboard and 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, port, and certificate name.

8c Click **OK**.

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

9a Click **Devices** > **Identity Servers** > **Servers** > **Edit** > **Local** > **User Stores** > **New**.

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

9c Update Identity Server.

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

Configuring Passwordless Authentication

Configure Advanced Authentication to perform the first-factor authentication through OAuth-based or plug-in-based approach. For information about differences between both approaches, see Implementation Approaches.

Configuring Passwordless Authentication using the OAuth-based Approach

Perform the following steps in Access Manager:

1 Configure an Advanced Authentication Generic class.

1a Click **Devices** > **Identity Servers** > **Edit** > **Local** > **Classes**.

1b Click **New** and specify the following details:

Display name: Specify a name for the class.

Java class: Select **Advanced Authentication Generic Class**. The Java class path is configured automatically.

1c Click **Next** > **Finish**.

2 Create a method for this class.

2a Click **Devices** > **Identity Server** > **Edit** > **Local** > **Methods** > **New**.

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

NOTE: If no chain is listed in **Advanced Authentication Chains**, create a chain in the Advanced Authentication server. If a chain is available in the Advanced Authentication server, but the chain is not listed 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 Click **Devices** > **Identity Servers** > **Edit** > **Local** > **Contracts** > **New**.

3b In **URI**, specify a value that uniquely identifies the contract from all other contracts. This value is used to identify this contract for external providers and is a unique path value that you create. For example, specify `/nam/AAgenericcontract` or `/mycompany/name/password/form`.

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

3d Click **Apply** > **OK**.

3e Update Identity Server.

NOTE: For a seamless Identity Server redirection, configure a CSP header by adding Advanced Authentication as an allowed source. For more information, see "Configuring the Custom Response Header for an Identity Server Cluster" in the *NetIQ Access Manager Appliance 5.0 Administration Guide* and TID.

Configuring Passwordless Authentication using the Plug-in-based Approach

Perform the following steps in Access Manager:

1 Configure an Advanced Authentication class.

1a Click **Devices** > **Identity Servers** > **Edit** > **Local** > **Classes**.

1b Click **New** and specify the following details:

Display name: Specify a name for the class.

Java class: Select an Advanced Authentication class except `Advanced Authentication Generic Class`. For example, select **SMS Class**.

The Java class path is configured automatically.

1c Click **Next** > **Finish**.

2 Create a method for this class.

2a Click **Devices** > **Identity Server** > **Edit** > **Local** > **Methods** > **New**.

2b Specify a name for this method.

2c Select **Identifies User**.

2d Under **Properties**, click **New**, and specify the following details:

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 Appliance 5.0 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 workaround this, proxy Identity Server and the Advanced Authentication server under the same domain name. See Configuring a FIDO U2F Class in the NetIQ Access Manager Appliance 5.0 Administration Guide.

3 Create a contract for the method.

3a Click **Devices** > **Identity Servers** > **Edit** > **Local** > **Contracts** > **New**.

3b In **URI**, specify a value that uniquely identifies the contract from all other contracts. This value is used to identify this contract for external providers and is a unique path value that you create. For example, specify `/nam/AApluginContract` or `/mycompany/name/password/form`.

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

3d Click **Apply** > **OK**.

3e Update Identity Server.

For more information about creating a contract, see “Configuring Authentication Contracts”in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

IMPORTANT: End users must enroll the methods for passwordless authentication. See “End Users Enrollment in the Advanced Authentication Self-Service Portal” on page 9.

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 “End Users Enrollment in the Advanced Authentication Self-Service Portal” on page 9.

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

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 Advanced Authentication portal for authenticator enrollments.

   For example:

   URL of the portal when it is 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) that you created in the previous step.
4. Using the dummy user’s account, 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 user’s phone's USB-C port or NFC reader and confirm the identity.

   If authentication succeeds, the integration is successful.

Verifying the OAuth-based Integration

Perform the following steps in Access Manager:

1. Create a class using Advanced Authentication Generic class.
2. Create a method with this class and select the required chain in **Advanced Authentication Chains**. For example, FIDO2.
3. Create a contract. Add the Advanced Authentication method that you created in the previous step.

4 Using the dummy user's account, 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 user's phone's USB-C port or NFC reader and confirm the identity.

   If authentication succeeds, the integration is successful.

   If authentication succeeds on the OSP page and you are redirected to Identity Server or protected resource, the integration is successful.

End Users Enrollment in the Advanced Authentication Self-Service Portal

To perform authentication with Advanced Authentication, end users must enroll all methods of an authentication chain that they can use for authentication.

Users must perform the following steps to enroll authenticators:

1. Access the Advanced Authentication Self-Service portal.

   URL of the portal when it is 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 to the FIDO2 method, select **FIDO2**, specify the email ID, and click **Save**.

   FIDO2 is displayed in the **Enrolled Authenticators** section.

Legal Notice