

Access Manager Business to Consumer Access Management

Traditional access management solutions are limited to control and manage employees' access within an organization. Organizations now provide more online services, thus the online presence of external stakeholders (consumers and partners) is growing. Organizations require to manage stakeholders efficiently. Organizations face many challenges in managing identities of consumers and partners and their access to services.

The following are some areas where most of the organizations face challenges:

- ♦ Ensuring a secure access because a username and password combination or traditional password based security has numerous vulnerabilities.
- ♦ Authenticating consumers based on federated protocols due to increase in the number of cloud-based services and Software-as-a-Service (SaaS) delivery models.
- ♦ Authenticating consumers based on their social media credentials.
- ♦ Providing seamless experiences across devices.
- ♦ Managing consumers' details.
- ♦ Providing protection and privacy to consumers' identity and personal information.

To overcome these challenges, Access Manager provides the following *business to consumer (B2C)* access management capabilities:

User-driven functionalities: Enables users to perform self-registration and manage their devices and applications without administrative intervention.

Better user experience: To provide a seamless access to applications from anywhere and from any device.

Intelligent and secure authentication mechanism: To provide a secure access to users by using methods such as risk-based authentication, identity proofing-email verification, device fingerprinting, and multi-factor authentication.

Social authentication: To grant access based on users' social media identity to reduce their overhead of managing multiple accounts, and for just-in-time provisioning.

APIs: To enable better integration with applications. These APIs enable programmatic interfaces to access administration and user data.

Data privacy: To ensure privacy of users' data by asking their consent and enabling them to select the information they want to share.

End user data control: To enable users to view, manage, and delete their applications and devices. It also enables users to manage their profile.

Access Manager User Portal is enhanced to support B2C access management capabilities. To provide B2C access management capabilities, Access Manager integrates with the following products:

- ♦ **NetIQ Self Service Password Reset 4.2 or later:** To enable customers and partners perform self-registration and to provide end user data control, such as change password and modify profile details.
- ♦ **NetIQ Advanced Authentication 5.6 Patch 1 or later:** To use the multi-factor authentication capability when a user tries to log in from an untrusted device.

The following diagram illustrates a common set of B2C access management capabilities of Access Manager:



1 An Example Scenario

Let us assume Acme Inc. is a life insurance provider that provides individual and group insurance products to its customers. It has nationwide agents that sell and service insurance products. It also sells insurance products through the online portal. It uses SaaS services such as ServiceNow, Salesforce, DocuSign, and LexisNexis to provide services to its consumers and agents.

Acme Inc. serves the following two types of online users:

- ♦ **Consumer:** A person who buys the insurance products. In this example, Carol is a consumer.
- ♦ **Insurance Agent:** A person who sells products of Acme Inc along with the products from other companies. An agent needs elevated privileges. In this example, Aaron is an agent. He needs privileges to access the information about commission details, view new products, view clients' insurance information, and access to additional services such as a service ticket in ServiceNow.

The Access Manager B2C portal caters to the following requirements of Aaron and Carol in this scenario:

Registration through any of the following ways:

- ♦ As a new user using the registration page
- ♦ As an agent
- ♦ Using social accounts

Agent Activation through the following way:

- ♦ Using B2C customer center to create an agent's username
- ♦ A verification code is sent to the agent's email ID
- ♦ The agent sets a password using username and verification code

Login through any of the following ways:

- ♦ Using the default login page
- ♦ Using social accounts
- ♦ Through a federated account
- ♦ Using an Advanced Authentication mechanism

Account Management to perform the following actions:

- ♦ View and delete applications
- ♦ View and edit profile details, such as name and phone number and preferences
- ♦ View and manage devices
- ♦ Manage passwords

Privacy and Consent Management to perform the following actions:

- ♦ Decide what information they want to share
- ♦ Manage privacy and consents
- ♦ Delete an account and erase all personal information

For information about how to configure B2C access management for this scenario, see [Business To Consumer Wizard: Sample Configuration](#).

2 Strategy for Deploying B2C

Access Manager B2C deployment consists of the following modules:

Self Service Password Reset: Enables consumers and partners perform self-registration, self-registration using social login information, account management (passwords, profile), and account deletion.

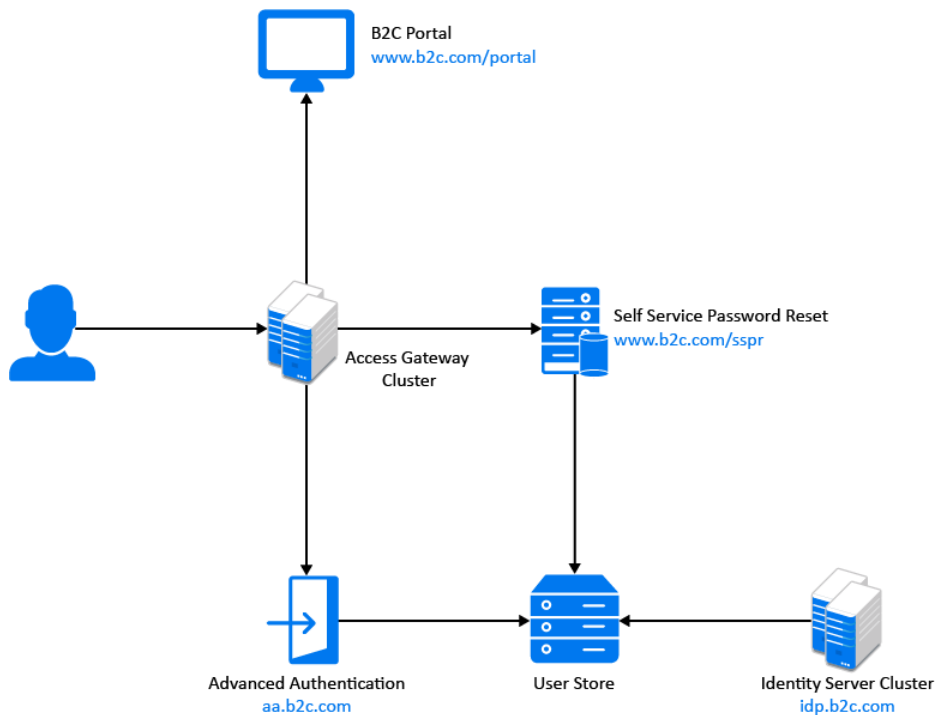
Advanced Authentication: Enables multi-factor authentication when a user tries to log in from an untrusted device.

B2C User Portal: This is the fully customized user portal.

Access Manager Access Gateway: Ties together the various components and provides a unified domain to the end user.

Access Manager Identity Server: Evaluates login risks and alters the level of authentication. Integrates with Advanced Authentication to provide a variety of authentication mechanisms

The following diagram illustrates how Self Service Password Reset and Advanced Authentication are integrated with Access Manager Appliance:



Deployment Workflow for B2C

You can use the following base URLs to deploy a standard B2C access management environment:

- ♦ **B2C login URL:** <https://www.b2c.com/portal>
- ♦ **User portal URL:** <https://idp.b2c.com:8443/nidp/portal>
- ♦ **Access Gateway hosting Self Service Password Reset URL:** <https://www.b2c.com/sspr/>
- ♦ **Access Gateway hosting Advanced Authentication URL:** <https://aa.b2c.com/account/basic>

IMPORTANT: Access Manager, Self Service Password Reset, and Advanced Authentication must use the same LDAP user store.

1. Set up the B2C login page.
See [Setting Up the B2C Login Page](#).
2. Configure Self Service Password Reset and Advanced Authentication servers.
See [Configuring Self Service Password Reset and Advanced Authentication](#).
3. Configure services for portal login page, Self Service Password Reset, and Advanced Authentication in Access Gateway.
See [Configuring Services for Login Page, Self Service Password Reset, and Advanced Authentication in Access Gateway](#).
4. Enable Self Service Password Reset and Advanced Authentication Servers integration in Identity Server.
See [Enabling Self Service Password Reset and Advanced Authentication Integration in Access Manager](#).

Specify Advanced Authentication server details in Identity Server only when you want to use authentication methods from Advanced Authentication.

5. Configure social authentication contracts. See [Configuring Social Authentication Contracts](#).
6. Configure device registration contract using an Advanced Authentication method for step-up authentication. See [Configuring a Device Registration Contract](#).
7. Configure to send email notifications when a user logs in using an unknown device. You can configure this option if you have configured a device registration contract. See [Configuring Email Server](#).

3 Setting Up the B2C Login Page

When you integrate Access Manager with Self Service Password Reset, it automatically enables the **Register** and **Forgot Password** links on the login page. However, you can configure the login page based on your requirements. You can choose the options and actions that are available for users on the login page.

Perform the following steps to set up the B2C login page:

- 1 Unzip `b2cFramework-1.0.zip`.
This file is available in the `/opt/novell/nids/lib/webapp/css/` folder of Access Manager Identity Server.
- 2 Locate `login_snippet.jsp` and `b2c_nam_login.jsp` and copy these files to the `/opt/novell/nids/lib/webapp/jsp/` folder of Access Manager Identity Server.
- 3 Locate `login_snippet.css` and copy this file to the `/opt/novell/nids/lib/webapp/css/` folder of Access Manager Identity Server.
- 4 Locate `example.html` and `example.css` and rename these to `index.html` and `index.css` respectively.
- 5 Open `index.html` and perform the following steps:
 - 5a Search for `<link rel="stylesheet" href="example.css">` and replace `example.css` with `index.css`.
 - 5b Search for `<script src="../login_snippet.js"></script>` and replace `login_snippet.js` with `https://idp.b2c.com:8443/nidp/jsp/login_snippet.jsp`.
 - 5c Search for `apiHost:` and replace `https://prvqenam660.namdom049.lab:8443/` with `https://idp.b2c.com:8443/`.
 - 5d (Optional) In the `login_snippet.jsp` file, configure parameter `loginUrl` with the new login URL. For example, `loginUrl: 'https://idp.b2c.com:8443/nidp/app/b2c_login'`.

IMPORTANT: This step is required only if the default authentication contract has two or more authentication methods configured. For example, if the default contract is a risk-based contract and it is configured to prompt for an additional authentication based on the risk, then configure this step.

- 6 Save `index.html`.
- 7 Host the following files on a web server or a Tomcat web application container:
 - ♦ `index.html`
 - ♦ `index.css`

To host these files, create a folder named `portal` in the root folder of the web server or in the tomcat container and copy these files to this folder.

- 8 Open `web.xml` located in Identity Server at `/opt/novell/nam/idp/webapps/nidp/WEB-INF/`.

9 In `web.xml`, enable the CORS filter by uncommenting the following filter configuration:

```
<filter>
    <filter-name>CorsFilterController</filter-name>
    <filter-
class>com.novell.nidp.servlets.filters.CorsFilterController</filter-class>
    </filter>
    <filter-mapping>
        <filter-name>CorsFilterController</filter-name>
        <url-pattern>*</url-pattern>
    </filter-mapping>
</filter>

<filter>
    <filter-name>CorsFilter</filter-name>
    <filter-class>org.apache.catalina.filters.CorsFilter</filter-
class>
    <init-param>
        <param-name>cors.allowed.origins</param-name>
        <param-value>*</param-value>
    </init-param>
    <init-param>
        <param-name>cors.allowed.methods</param-name>
        <param-value>GET,POST,HEAD,OPTIONS,PUT</param-value>
    </init-param>
    <init-param>
        <param-name>cors.allowed.headers</param-name>
        <param-value>Content-Type,X-Requested-With,accept,Origin,Access-
Control-Request-Method,Access-Control-Request-Headers</param-value>
    </init-param>
    <init-param>
        <param-name>cors.exposed.headers</param-name>
        <param-value>Access-Control-Allow-Origin,Access-Control-
Allow-Credentials</param-value>
    </init-param>
</filter>
<filter-mapping>
    <filter-name>CorsFilter</filter-name>
    <url-pattern>*</url-pattern>
</filter-mapping>
```

10 Add the following snippet:

```
<servlet>
    <servlet-name>B2CLoginServlet
    </servlet-name>
    <display-name>B2C Login Servlet
    </display-name>
    <jsp-file>/jsp/b2c_nam_login.jsp
    </jsp-file>
</servlet>
<servlet-mapping>
    <servlet-name>B2CLoginServlet
    </servlet-name>
    <url-pattern>/app/b2c_login
    </url-pattern>
</servlet-mapping>
```

- 11 Add `b2c_nam_login.jsp` to the list of JSP in the `param-value` of the `name>nidpJspFilter` filter.
- 12 Restart Identity Server.
- 13 Ensure that you can access the B2C login page now at `http(s)://<web server IP address where index.html is hosted>/portal/index.html` and that the page contains a login form.

For more customization options, locate `Login Snippet.pdf` in the files extracted from `b2cFramework-1.0.zip`. Open it to find further steps to customize the B2C login page.

4 Configuring Self Service Password Reset and Advanced Authentication

- ♦ [Section 4.1, “Configuring Self Service Password Reset for B2C,” on page 7](#)
- ♦ [Section 4.2, “Configuring Advanced Authentication for B2C,” on page 11](#)

4.1 Configuring Self Service Password Reset for B2C

In the B2C access management deployment, the following requirements are achieved using Self Service Password Reset:

- ♦ User account creation during self-registration
- ♦ User account creation during social registration
- ♦ User account activation for the agent registration
- ♦ Password recovery for user accounts
- ♦ Profile update for user accounts
- ♦ Account deletion
- ♦ Change password

Perform the following tasks in Self Service Password Reset to achieve these requirements:

1. Log in to Self Service Password Reset as an administrator.
2. In the toolbar, click your username and select **Configuration Editor**.
3. Create a general profile for self-registration.
For more information, see [Enabling Self-Registration](#).
4. Create a social profile for social registration.
For more information, see [Enabling Self-Registration Using Social Login Information](#).
5. Enable and edit the **User Activation** profile for agent registration.
For more information, see [Configuring the User Activation Profile Module \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14knuop.html\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14knuop.html).
6. Enable and edit the **Forgotten Password** profile to enable the users to reset password and login again.
For more information, see [Configuring the Update Profile Module \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b1ggnpqg.html\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b1ggnpqg.html).
7. Enable and edit the **Update Profile** profile to enable the users to update their profiles.
For more information, see [Configuring the Update Profile Module \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14knvb3.html\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14knvb3.html).

8. Edit the **Delete Account** profile to enable users to delete their profile.
For more information, see [Enabling User Deleting Capabilities](#).
9. Enable the **Change Password** profile to enable users to change their passwords. This is the default profile for change password. You can edit this profile to change the default behavior.
For more information, see [Configuring the Change Password Module \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14knh9k.html\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14knh9k.html).
10. Click **Modules > Public > New User Registration > New User Settings** and select **Enabled**.
11. Click **Security > Web Security** and specify the following URLs in **Redirect Whitelist**:
 - ♦ `https://www.b2c.com`
 - ♦ `https://idp.b2c.com:8443/nidp`
12. You can define various URLs in Self Service Password Reset configuration to redirect the user to a logical page after the completion of each task.
To define these URLs, click **Settings > Application > Application**, and set up the following URLs:
 - ♦ Set up a **Site URL**. For example, `https://www.b2c.com/sspr`
 - ♦ Set up a **Forward URL**. For example, `https://www.b2c.com/portal/index.html`
 - ♦ Set up a **Logout URL**. For example, `https://www.b2c.com/AGLogout`
 - ♦ Set up a **Home URL**. For example, `https://idp.b2c.com:8443/nidp/portal`

4.1.1 Enabling Self-Registration

To enable user self-registration, you must create a profile in Self Service Password Reset.

Perform the following steps to create a profile:

- 1 Create a new **New User Profile** profile using a unique profile name. For example, General.
- 2 Click **Modules > Public > New User Profile > General**.
- 3 Edit **Creation Context** in the General profile to match the context in the LDAP directory where users are created. For example, `ou=users,o=novell`.
- 4 Edit the form based on the information that you require from users.

A standard form contains the following fields:

Name	Label
<code>cn</code>	User Name
<code>givenName</code>	First Name
<code>sn</code>	Last Name
<code>mail</code>	Email
<code>mobile</code>	Mobile

NOTE: If your LDAP store is Active Directory, `cn` will be `sAMAccountName`.

- 5 Delete the default definition in **LDAP Entry ID Definition** if `cn` is part of the user configured in the previous step.

- 6 (Optional) You can select **Enable New User Email Verification** and **Enable New User SMS Verification** based on your verification requirement.
- 7 Set up **After Registration Redirect URL** for the **New User Registration** general profile. For example, `https://www.b2c.com/portal`.
- 8 If the Self Service Password Reset configuration for forgotten password is challenge/response then **After Registration Redirect URL** is the Access Gateway URL. For example, `https://www.b2c.com/sspr/private/setup-responses`.
- 9 Select **Prompt User for Password** to prompt the user to provide a password during registration.
- 10 Now, users can register themselves using the `/sspr/public/newuser/profile/General` URL.

For more information about how to configure profiles in Self Service Password Reset, see [Configuring Profiles \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t41w0qfruh1o.html\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t41w0qfruh1o.html) in the **Self Service Password Reset 4.2 Administration Guide**.

4.1.2 Enabling Self-Registration Using Social Login Information

Perform the following steps to configure Self Service Password Reset to enable user registration using social networking accounts:

- 1 Create a new **New User Profile** profile using a unique profile name. For example, Social.
- 2 Edit **Creation Context** in the social profile to match the context in the LDAP directory where users are created.
For example, `ou=users,o=novell`.
- 3 Edit the form based on the information that you require from user. A standard form contains the following fields:

Name	Label
cn	User Name
displayName	Full Name
sn	Last Name
mail	Email
carLicense	Unique ID

NOTE: If your LDAP store is Active Directory, then `cn` will be `sAMAccountName`.

- 4 Delete the default definition in **LDAP Entry ID Definition** if `cn` is part of the form configured in Step 3.
- 5 (Optional) You can select **Enable New User Email Verification** and/or **Enable New User SMS Verification** based on your verification requirement.
- 6 Deselect **Prompt User for Password** to ensure that the user is not prompted for password.
- 7 Click **Settings > Web Services > REST Services**.
Perform the following steps in **REST Services**:
 - 7a Select **Enable External Web Services**.
 - 7b Click on **Add Value** in **External Web Services Secret**.

- 7c** Specify a name for the new password. For example, NAMSECRET.
- 7d** Specify a password and click **Store Password**. For example, pass@123.

IMPORTANT: This name and password is used when you configure Access Manager to integrate with Self Service Password Reset. Specify name in **API Username** and password in **API Password** while specifying the Self Service Password server details in Identity Server.

See [Configuring Self Service Password Reset Server Details in Identity Server](#).

- 7e** Click **Usage** and select **Signing Form Service - /signing/form** and **Health Service - /health**.



- 7f** Click **OK**.
- 7g** Log in to Access Manager as an administrator. Navigate to **Identity Server > Shared Settings > Self Service Password Reset > Integration Links**. Specify a path for profile in **Auto Registration URL**. For example, /public/newuser/profile/Social.

- 8** Now, users can register themselves using the /sspr/public/newuser/profile/Social URL.

For more information about how to register social users using Self Service Password Reset, see [Creating Accounts for Social Users in Self Service Password Reset Using the New User Registration Module \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t43milg959i5.html#t43mjeqte4xz\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t43milg959i5.html#t43mjeqte4xz) in the [Self Service Password Reset 4.2 Administration Guide](#).

4.1.3 Enabling User Deleting Capabilities

Configure the **Delete Account** module in Self Service Password Reset. This enables users to delete their account information stored in Access Manager. When users delete their own accounts from the B2C portal, the requests are sent through REST API to Access Manager. This configuration is required when you want to delete the complete user history and device registration is configured in the Access Manager contract.

For information about how to enable user delete capabilities, see [Deleting User Accounts in Access Manager from the Delete Account Module \(https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t41u798dzatw.html#t43v4wntk846\)](https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t41u798dzatw.html#t43v4wntk846) in the [Self Service Password Reset 4.2 Administration Guide](#).

Ensure that you perform the following additional steps:

- ♦ Enable the **Delete LDAP Entry** option.
- ♦ To logout the user from Access manager after deletion of the user, set up **Next URL** for **Delete Account**. For example, <https://www.b2c.com/AGLogout>.

4.2 Configuring Advanced Authentication for B2C

IMPORTANT: You must configure the Advanced Authentication server before creating an Advanced Authentication class in Access Manager. See “[Configuring Advanced Authentication Server](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

To configure Advanced Authentication, perform the following steps:

- 1 Log in to Advanced Authentication Administrative Portal.
- 2 Create an advanced authentication method in Advanced Authentication Server.
For example, select the security question method. See “[Configuring Authentication Methods](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.
- 3 Create a chain named b2c. Assign the security question method created in previous step to the b2c chain. Ensure that all users are assigned to this chain. Assign the b2c chain to the default Access Manager event created in Advanced Authentication.
For more information about how to create and assign a chain, see [Creating a Chain \(https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/creating_chain.html\)](https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/creating_chain.html).
- 4 Assign the b2c chain to the default Access Manager event by moving the b2c chain from **Available** to **Used**.
- 5 Add the Access Manager Identity Server endpoint to the Access Manager event so that the Identity Server endpoint is white listed for the Access Manager event. You can perform this step only when the Advanced Authentication server details are specified in Identity Server.
For more information about configuring Advanced Authentication, see “[Multi-Factor Authentication Using Advanced Authentication](#)”.

5 Configuring Services for Login Page, Self Service Password Reset, and Advanced Authentication in Access Gateway

Login Page, Self Service Password Reset, and Advanced Authentication are configured as protected resources in Access Gateway to enable SSO.

- ♦ [Configuring the B2C Login Page as a Service in Access Gateway](#)
- ♦ [Configuring SSO to Self Service Password Reset Through Access Gateway](#)
- ♦ [Configuring SSO to Advanced Authentication Through Access Gateway](#)

5.1 Configuring the B2C Login Page as a Service in Access Gateway

- 1 Create a reverse proxy named b2cproxy in Access Gateway. Specify a **Secure Port**. For example, 443. Assign a wild card certificate as Server Certificate.

For information about how to create a reverse proxy, see “[Managing Reverse Proxies and Authentication](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

NOTE: You can specify any value in **Secure Port**, but you must configure the B2C access management deployment URLs in Access Gateway accordingly.

- 2 Create a proxy service named `b2cproxyservice` and provide the published DNS name as `www.b2c.com`.

For information about how to create and configure a proxy service, see “[Creating a Proxy Service](#)” and “[Configuring a Proxy Service](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 3 Specify the IP address of the server that is hosting `index.html`.

For information about `index.html`, see [Setting Up the B2C Login Page](#).

- 4 Create a protected resource to the proxy service created in [Step 2](#) and specify `/*` in **URL Path** while creating the protected resource.

Do not assign a contract to this protected resource. This enables users with self-registration and password reset capabilities.

For information about how to create a protected resource, see “[Setting Up a Protected Resource](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

Now, you can access the login page as `https://www.b2c.com/portal`.

5.2 Configuring SSO to Self Service Password Reset Through Access Gateway

- 1 Create a path based multi-homing proxy service for the reverse proxy `b2cproxy` created in [Step 1 on page 11](#). Specify `/sspr` in **Path** while creating the proxy service.

For information about how to create and configure a proxy service, see “[Creating a Proxy Service](#)” and “[Configuring a Proxy Service](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 2 Create a protected resource for the proxy service created in the [Step 1](#). Specify `/sspr/*` in **URL Path** while creating the protected resource.

Do not assign a contract to this protected resource. This enables users with self-registration and password reset capabilities.

For information about how to create a protected resource, see “[Setting Up a Protected Resource](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 3 Create another protected resource for the proxy service created in [Step 1](#). Specify `/sspr/private/*` in **URL Path** while creating the protected resource. Assign the **Secure Name/Password - Form** contract to this protected resource so that only authenticated users can access this protected resource. Ensure that **Satisfiable by Contracts of Equal or higher level** is enabled for the Secure Name/Password - Form Contract.

For information about how to create a protected resource, see “[Setting Up a Protected Resource](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 4 Create an identity injection policy and assign it to the protected resource created in [Step 3](#). Choose **Inject into Authentication Header** in **Action** while creating the identity injection policy.

For more information about how to create and assign an identity injection policy, see “[Identity Injection Policies](#)” and “[Assigning an Authorization Policy to a Protected Resource](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

Perform the following steps when you configure the authentication header policy:

- 4a In **User Name**, select **Credential Profile** and select **LDAP User Name** (the `cn` attribute of the user) in **LDAP Credentials**.

For more information about how to configure the authentication header policy, see “[Configuring an Authentication Header Policy](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 4b In **Password**, select **Credential Profile** and select **LDAP Password** in **LDAP Credentials**.

For more information about how to configure the authentication header policy, see “[Configuring an Authentication Header Policy](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

The following diagram shows how the identity injection policy appears in Access Gateway:

Now, users can access the following URL using Self Service Password Reset:

- **Authenticated Users:** <https://www.b2c.com/sspr/private>
- **Public Users:** <https://www.b2c.com/sspr/public/newuser/profile/General>

The following diagram shows how the protected resources appear in Access Gateway after configuration:

Protected Resource List							
New...	Delete	Enable	Disable				
<input type="checkbox"/>	Name	Enabled	URL Paths	Authentication Procedure	Authorization	Identity Injection	Form Fill
<input type="checkbox"/>	public	✓	1 Paths	[None]	[None]	[None]	[None]
<input type="checkbox"/>	sspr_private	✓	1 Paths	Secure Name/Password - Form	[None]	sspr_ii	[None]
<input type="checkbox"/>	sspr_public	✓	1 Paths	[None]	[None]	[None]	[None]
			<input type="text" value="/sspr/private/*"/>				

5.3 Configuring SSO to Advanced Authentication Through Access Gateway

To configure SSO to the Advanced Authentication enrollment page, you must configure several settings in Access Gateway and in Advanced Authentication.

Advanced Authentication must be enabled for basic authentication to achieve SSO using Access Gateway. Advanced Authentication processes only the HTTP Authorization header for incoming requests that include /basic in the path, for example: <https://aa.b2c.com/account/basic>. To enable basic authentication, perform the following steps:

Configuring Advanced Authentication

- 1 Log in to Advanced Authentication Administration Console and ensure that an **Authentication** chain exists with the LDAP Password method.
- 2 Edit the Authentication chain mentioned in [Step 1](#) to assign the chain to all users.
- 3 Set the **Allow basic authentication** option to **ON** for the **Authenticators Management** event.

Basic authentication is supported for one event type (Authentication Management event) and three methods: Password (PIN), LDAP Password, and HOTP.

- 4 Create an authentication chain using any of these supported methods. For example, select the LDAP Password method while creating the chain.

For more information, see [Authenticators Management \(https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/configuring_event.html#b1og8fp4\)](https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/configuring_event.html#b1og8fp4) in the [Advanced Authentication - Administration](#) guide.

- 5 Go to **Events**, select the **Authenticators Management** event, and add the chain created in the previous step.

Configuring Access Gateway

You can configure Access Gateway to accelerate a back-end web server and inject users' credentials into the Authorization HTTP header. This enables SSO to any web server that supports basic authentication. This Authorization HTTP header is a standard header that can include a Base64 encoded version of username:password. In the case where Advanced Authentication is the back-end web server, it expects a special formatting of the Authorization header. For example, <username>:<password>:1. A virtual attribute will be used to provide this formatting.

- 1 Set up Access Manager to inject the non-standard Authorization HTTP header.

To do this, create a virtual attribute based on the users' cn and manipulate the data with JavaScript.

Perform the following steps to create and configure the virtual attribute:

- 1a Click **Devices > Identity Server > Shared Settings > Virtual Attributes > Virtual Attribute > +**.
- 1b Specify a name such as `va-adv-auth` and description for the virtual attribute.
- 1c Under **Step 1 : Provide input parameters**, specify a name for the attribute and select **cn** as **Parameter Value**.
- 1d Under **Step 2 : Provide a modification function**, select **Advanced JavaScript**.
- 1e Specify the following JavaScript:

```
function main (P1){
    return P1+":LDAP_PASSWORD:1"
}
```
- 1f Click **OK**.
- 1g Update Identity Server.

For more information about virtual attributes, see "[User Attribute Retrieval and Transformation](#)" in the [NetIQ Access Manager Appliance 4.5 Administration Guide](#).

- 2 Create an Identity Injection policy that injects the above virtual attribute value as part of the username, with the users' password as `password`. This policy will later be applied to the protected resources associated with the Advanced Authentication enrollment portal page.
 - 2a In Administration Console Dashboard, click **Policies > Policies**.
 - 2b Select the policy container and click **New**.
 - 2c Specify a name for the policy, select **Access Gateway: Identity Injection** for the type of policy, then click **OK**.
 - 2d Select **1** in **Priority**.
 - 2e In **Actions**, click **New**, then select **Inject into Authentication Header**.

2f In **User Name**, select **Virtual Attributes** and the attribute created in [Step 1 on page 14](#).

2g In **Password**, select **Credential Profile** and in **LDAP Credentials**, select **LDAP Password**.

2h Click **OK**.

For more information about Identity Injection policies, see “[Identity Injection Policies](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

The following diagram shows how the identity injection appears in Access Gateway after configuration:

Edit Rule: aa_ii - Rule 1

Type: Access Gateway: Identity Injection

Description:

Priority: 1

Actions

New ▾

Do Inject into Authentication Header

User Name: Virtual Attribute ▾ : va-adv-auth ▾ Refresh Data Every: Session ▾

Password: Credential Profile ▾ : LDAP Credentials:LDAP Password ▾

Multi-Value Separator: , ▾

DN Format: LDAP (ex, cn=jsmith,ou=Sales,o=Novell) ▾

Changes made on this panel must be applied from the [Policies](#) Panel.

OK Cancel

3 Accelerate the Advanced Authentication enrollment server by using Access Gateway.

For example, set up a domain based multi-homed proxy for the Advanced Authentication enrollment server.

1. When you configure this proxy, specify **aa.b2c.com** in **Published DNS Name** and Advanced Authentication server IP address in **Web Server Address**.
2. Create a protected resource for the path (can be /* or specifically /account/basic) and assign the Secure Name/Password - Form contract to this protected resource, so that only authenticated users can access this protected resource. Assign the Identity Injection policy created in [Step 2](#) to this protected resource.
3. Update Access Gateway after applying these changes.

For more information, see “[Configuring Protected Resources](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

The following diagram shows how the protected resource is displayed in Access Gateway after configuration:

Protected Resource List							
New...	Delete	Enable	Disable				
<input type="checkbox"/>	Name	Enabled	URL Paths	Authentication Procedure	Authorization	Identity Injection	Form Fill
<input type="checkbox"/>	prot	✓	1 Paths ▾	Secure Name/Password - Form	[None]	aa_ii	[None]
<input type="checkbox"/>	public	✓	1 Paths ▾ /account/basic	[None]	[None]	[None]	[None]

4 Now, users can access the Advanced Authentication proxy URL (<https://aa.b2c.com/account/basic>). Also, users can see their Advanced Authentication enrollment page after logging into Identity Portal.

6 Enabling Self Service Password Reset and Advanced Authentication Integration in Access Manager

To enable integration with Self Service Password Reset and Advanced Authentication, you must specify server details for these products in Access Manager Identity Server.

- ♦ [Section 6.1, “Configuring Self Service Password Reset Server Details in Identity Server,” on page 16](#)
- ♦ [Section 6.2, “Configuring Advanced Authentication in Identity Server,” on page 17](#)

6.1 Configuring Self Service Password Reset Server Details in Identity Server

Perform the following steps to specify the Self Service Password Server details:

- 1 Click **Devices > Identity Server > Shared Settings > Self Service Password Reset**.
- 2 Select **Integrate with Self Service Password Reset (SSPR)**.
- 3 Specify the following details under **Server Configuration**:

Field	Description
Published SSPR URL	Select http or https and specify the Self Service Password Reset server’s IP address or DNS name with the port number. If Self Service Password Reset is configured behind Access Gateway, then specify Access Gateway's Published URL for Self Service Password Reset. For example, specify <code>https://www.b2c.com/sspr/</code> .
API User Name	Protected web services that require authentication through a user name and password use the secret name as user name. The secret name is generated while configuring the Self Service Password Reset server. For example, specify <code>NAMSECRET</code> in API User Name .
API Password	Protected web services that require authentication through a user name and password use a secret key as password. The secret key is generated while configuring the Self Service Password Reset server. For example, specify <code>pass@123</code> in API Password .

- 4 Click the **+** icon under **Integration Links** to see URLs associated with the specified Self Service Password Reset server.

Integration Links displays default URLs. These URLs must be modified to match the URLs specified on the Self Service Password Reset server. If you modify the integration links in the Self Service Password Reset server, specify the same integration links in **SSPR Portal Links** and **REST APIs**. The values specified in **Integration Links** come after Published SSPR URL to form a destination path.

IMPORTANT: In some of the default URLs, forwardURLs are appended to ensure that the user is forwarded to correct URLs after performing the corresponding tasks.

Field	Description
User Profile URL	If a forwardURL is provided, the user is redirected to that URL after updating user profile in user portal. For example, if User Profile URL is set to <code>/private?forwardURL=https://idp.b2c.com:8443/nidp/portal</code> , the user is directed to that URL after profile update.

Field	Description
New Registration URL	If a forwardURL is provided, the user is redirected to that URL after registering as a new user on B2C portal page. For example, if User Registration URL is set to /private?forwardURL=https://idp.b2c.com:8443/nidp/portal, the user is directed to that URL after registration.
Auto Registration URL	It automatically registers users when users log in using social authentication. It compares the user specified attributes to the stored attributes. Specify /public/newuser/profile/Social.
Forgot Password URL	<p>If a forwardURL is provided, the user is redirected to that URL after password reset. For example, if Forgot Password URL is set to /private?forwardURL=https://idp.b2c.com:8443/AGLogout, then the user is directed to that URL after the user resets password.</p> <p>NOTE: Forgot Password URL is not accessible if Logout after password change is enabled in the Change Password module of Self Service Password Reset.</p>
Health API	It is used to obtain the health status of the Service Password Reset server. The default URL is /public/rest/health.
Back Channel Request Signing API	Access Manger uses this API to obtain information from Self Service Password Reset server. The default URL is /public/rest/signing/form.
Connection Timeout	Time limit to establish the connection with Self Service Password Reset server. The connection must establish within the specified time.
Read Timeout	Time limit to obtain the information from Self Service Password Reset after establishing the connection. Access Manager must obtain information within the specified time.

IMPORTANT

- ♦ Ensure that these URLs are specified in the Self Service Password Reset white list. To specify these URLs in white list, navigate to **Self Service Password Reset > Settings > Security > Web Security > Whitelist**.
- ♦ If a forwardURL is not provided, then the default URLs are used. To see default URLs, navigate to **Self Service Password Reset > Settings > Application > Forward URL**.

5 Click **Apply Changes**.

6.2 Configuring Advanced Authentication in Identity Server

Perform the following steps to configure Advanced Authentication server details in Identity Server:

- 1 Click **Devices > Identity Server > Shared Settings > Advanced Authentication**.
- 2 Specify aa.b2c.com and 443 in **Server Domain**.

For more information, see “[Configuring Advanced Authentication Server](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

After specifying the Advanced Authentication server details in Identity Server, an Identity Portal endpoint is automatically created in Advanced Authentication. Perform the following steps to add this endpoint to the white list:

- 1 Log in to Advanced Authentication Administration Portal.
- 2 Navigate to **Advanced Authentication Administration > Events > Authenticators Management**.
- 3 In **Authenticators Management**, the Identity Portal endpoint is listed as Identity Portal's hostname. Move the Identity Portal's hostname from **Available** to **Used**.
- 4 Click **Save**.

7 Configuring Social Authentication Contracts

You can configure a social authentication contract to allow users to log in using their social login information.

Perform the following steps to create a social authentication contract:

- 1 Perform the following steps to create a social authentication class:
 - 1a Log in to Administration Console of Access Manager.
 - 1b Click **Devices > Identity Servers > Edit > Local > Classes**. Select **New** to add a new class.
 - 1c Specify a name for the class.
 - 1d Select **Social Auth Class** from the **Java Class** list and click **Next**.
 - 1e Select the **Identify User Locally**, **Auto Provision User Using** and **SSPR** options to automatically provision a social user to a local user using Self Service Password Reset.
 - 1f Select the following **Social Attributes** and their equivalent **Local Attributes**:

Social Attribute	Local Attribute
Email	Ldap Attribute:mail [Ldap Attribute Profile]
FirstNamePlusLastName	Ldap Attribute:cn[Ldap Attribute Profile] For Active Directory, select LdapAttribute:sAMAccountName [LdapAttribute Profile]
Uniquelid	Ldap Attribute:carLicense [Ldap Attribute Profile]

IMPORTANT: Select only those social attributes that are provided by social providers. In addition, the social attribute must be mapped to the correct type of local attribute. For example, provisioning will not occur in the following scenarios:

- ♦ If you use Facebook or Google+ as your authentication provider and select **DisplayName** as **Social User Attribute**. Because these providers do not have the **DisplayName** attribute.
- ♦ If you use Twitter as your authentication provider and select **Email** as **Social User Attribute**. Because Twitter does not provide email.
- ♦ If more than one social authentication providers are configured and **Local Attribute** is a single-valued attribute. Here, the **Local User LDAP attribute** must be multi-valued attribute to store the social attributes corresponding to each social provider.

- 1g Select **User Identifier** adjacent to the mapping that will be used to identify the user.

For more information about how to create and configure a social authentication class, see [“Configuring the Social Authentication Class”](#) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 2 Create a method in Identity Server. When you configure this method, select the social authentication class created in the previous step from the **Class** list.

For more information about how to create and configure a method, see [“Configuring Authentication Methods”](#) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 3 Create a contract in Identity Server. When you configure this contract, add the method created in the previous step from **Available methods** to **Methods**. Ensure that you select **Satisfiable by a contract of equal or higher level**. So that this contract is satisfied by the device registration contract that you will create in [Configuring a Device Registration Contract](#).

For more information about how to create and configure a contract, [“Configuring Authentication Contracts”](#) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 4 If the user store is eDirectory, configure a **passwordFetch** method pointing to that directory and add the **passwordFetch** method to this contract.

IMPORTANT: If the user store is eDirectory, configure the **passwordFetch** class in each social contract to enable SSO for users to the following pages:

- ♦ The Profile page in Self Service Password Reset
- ♦ The Enrollment page in Advanced Authentication

If the user store is not eDirectory, users cannot view these pages.

8 Configuring a Device Registration Contract

You can configure a contract that allows users to register their devices after authentication. You can also configure an Advanced Authentication method for additional authentication.

Perform the following steps to enable device registration capability:

- 1 Create a risk-based policy and assign it to a risk-based authentication class.

For information about how to create and configure a risk-based policy, see [“Configuring a Risk Policy”](#) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 2 Create a Device Fingerprinting Rule and assign it to the risk-based policy created in the previous step. Select the following options when you configure rule definitions:

Store Fingerprint in: Select **Server** to store the fingerprint in the configured risk-database. You can use this option only in risk-based post-authentication scenarios.

To store the fingerprint in a risk-database, you must enable storing the user history in the **User History** tab.

See [“Enabling User History”](#) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

Prompt User Consent: Select this option to allow users to provide their consent before storing the device fingerprint.

Send Email Notification: Select this option to send an email to a user when the user logs in using an unknown device.

For more information about how to specify the email server details, see [“Email Server Configuration”](#) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

For more information about how to create and configure a rule, see “[Configuring Rules](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 3 (Optional) In the risk-based policy, configure additional authentication using an Advanced Authentication method.

For more information, see “[Configuring Authentication Methods](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

To set the enrollment URL during the additional authentication, add the following Advanced Authentication Enrollment URL property in the advanced authentication method:

Property Name: ENROLLURL

Property Value: https://aa.b2c.com/account/basic

- 4 Create a method for the risk-based authentication class.

For more information, see “[Configuring a Method for an Authentication Class](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

- 5 Create a contract for the risk-based authentication class. When you configure this contract, select the first method as **Secure Name/Password - Form**, and select the second method as risk-based method created in previous step. In addition, ensure that you select the **Satisfiable by a contract of equal or higher level** option.

For more information, see “[Configuring a Contract for an Authentication Class](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

When this contract is configured, users can register their device, view the registered devices, and delete these devices.

9 Configuring Email Server

You can configure Access Manager if you want to send email notifications to users when they log in using a new device. To enable this capability, specify email server details in the Administration Console Dashboard. In addition, you must select **Send Email Notification** option while configuring the Device Fingerprinting Rule.

For more information about how to specify the email server details, see “[Email Server Configuration](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

10 Branding and Customizing

- ♦ [Section 10.1, “Branding and Customizing Access Manager,” on page 20](#)
- ♦ [Section 10.2, “Customizing Self Service Password Reset,” on page 21](#)
- ♦ [Section 10.3, “Customizing Advanced Authentication,” on page 21](#)

10.1 Branding and Customizing Access Manager

You can change the default branding of the user portal page using the **Branding** option on Administration Console Dashboard. For more information, see “[Branding of the User Portal Page](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

To perform complex customization, you can edit the JSP file.

For information about Identity Server customization, see “[Customizing Identity Server](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

For information about Access Gateway customization, see “Email Server Configuration” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

10.2 Customizing Self Service Password Reset

You can customize the theme of Self Service Password Reset. See the following resources for instructions:

Customizing the Theme of Self Service Password Reset (<https://www.netiq.com/documentation/self-service-password-reset-45/sspr-adminguide/data/b14kmw4t.html>)



http://www.youtube.com/watch?v=bqX-ymk_8ZU

10.3 Customizing Advanced Authentication

You can customize the logo for the Administration and Self-Service portal in Advanced Authentication. You can also set an alternate text instead of an image as logo.

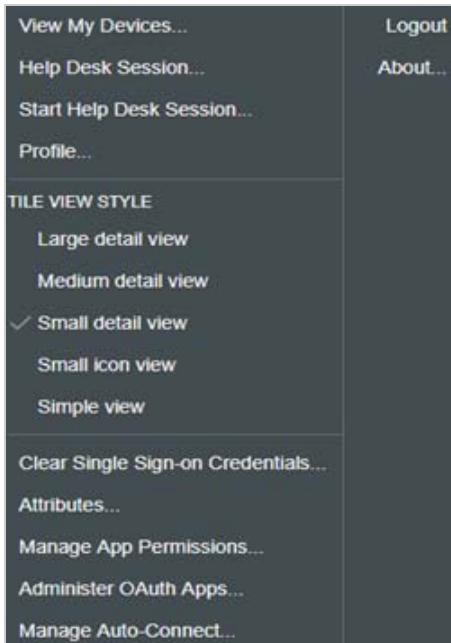
For more information, see *Configuring Policies* (https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/configuring_policy.html#b1oqe99n) in the *Advanced Authentication - Administration Guide* (<https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/bookinfo.html>).

11 Validating Deployment

After completing the portal deployment, validate the following scenarios:

- ♦ **Agent registration:** Agent registration is achieved through visiting the <https://www.b2c.com/sspr/public/activate> link.
 1. The B2C customer center creates an agent username and assigns appropriate agent-specific rights to this username.
 2. Then the customer center sends an email to the agent’s email ID with this pre-created username. The agent needs to click the link <https://www.b2c.com/sspr/public/activate> to register to the agent account.
 3. After clicking the link and providing the username, the agent is prompted to specify a code for validating the account. The agent gets the required code through an email.
 4. After specifying the correct code, the agent is asked to set the password. After setting the password, the agent registration is complete. The agent can log in to the portal by specifying the username and password.
- ♦ **User self-registration:** A user can click the **Register** link in the login page (<https://www.b2c.com/portal>) and perform self-registration.
- ♦ **Social registration:** A user can click the favorite social provider link on the login page to achieve this.
- ♦ **Login as an agent or a self-registered user:**
 1. A registered agent or a self-registered user can provide username and password in the Login form on the login page to achieve this.
 2. For the first time login, a device is detected as a new device and prompted for second factor authentication.

3. After the second factor authentication is completed, the user is prompted with a Consent screen to allow or deny storing the device details.
 4. If the user selects to allow consent, the device details are stored in Access Manager. The next login from the same device does not prompt for second factor authentication.
- ♦ **Login as a social profile registered user:** The registered social user can click the social provider link in the login page to achieve this.
 - ♦ **User account self-management:** After login, the user is redirected to the User Portal. When the user clicks the username in the upper right corner, a menu similar to the following displayed:



The user can perform the following actions using this menu:

Click	To
Profile	View and edit profile, change password, set security questions and answers to recover forgotten password, and delete the account.
View My Devices	View and delete devices.
View My Devices	Enrollment to the new authentication method.
Manage Auto-Connect	View SAML 2.0 service providers and shared attributes.
Manage App Permissions	View OAuth 2.0 resources, shared scopes, and attributes.

12 Progressive Profiling

Progressive profiling helps you improve the user experience by gathering the user’s data gradually. Instead of a huge overwhelming form asking for all details, progressive profiling uses shorter and multiple sequential forms. This approach focuses on collecting only the important information from a user that is required at that moment.

With progressive profiling, you understand your users more accurately, about what information they can share comfortably.

You can ask a user to provide only the minimal details, such as name and email address, during the registration. The type of information provided during registration can vary depending on the type of information or service for which a user is requesting.

The user can provide more details over time as and when performing a specific action. This in turn simplifies the registration and login experiences for users.

For example,

User Action	Information Required from a User
Registration	Name and Email Address
Search for an insurance policy	Contact number and city
Buy an insurance	Date of birth and postal address

To configure progressive profiling for this example scenario, perform the following tasks in Self Service Password Reset:

- ♦ [Configuring the New User Registration Module](#)
- ♦ [Configuring Profiles](#)
- ♦ [Integrating Profiles with Protected Resources or Custom Portals](#)

12.1 Configuring the New User Registration Module

- 1 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
- 2 In the toolbar, click your name.
- 3 Click **Configuration Editor > Modules > Public > New User Registration > New User Profile > default**.
- 4 Configure the first name, last name, and email ID.
- 5 Enable the New User Registration module:
 - 5a Click **Modules > Public > New User Registration > New User Settings**.
 - 5b Select **Enable New User Registration**.
- 6 In the toolbar, click **Save changes**.

With this configuration, a user needs to provide only the first name, last name, and email ID while registering.

12.2 Configuring Profiles

Perform the following actions:

1. Modify the default profile to collect LDAP attributes for the user's contact number and the name of the city. If a user has already provided this information, the user does not require to provide it again.

See [Modifying the Default Profile](#).

2. Add another profile to collect LDAP attributes for the user's date of birth and postal address.

See [Adding a New Profile](#).

This configuration enables you with collecting the relevant user information as and when required. The user does not need to share the date of birth and postal address while performing a search for an insurance policy. When the user decides to buy a policy, you collect this information.

12.2.1 Modifying the Default Profile

- 1 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
- 2 In the toolbar, click your name.
- 3 Click **Configuration Editor** > **Modules** > **Authenticated** > **Update Profile** > **Update Profile Profiles** > **default**.
- 4 In **LDAP Search Filter**, specify `(&((!(mobile=*))(!(city=*))((!(homepostaladdress=*))(!(Version=*)))))`.
- 5 In the **Update Profile Form** section, add contact number and city.
- 6 In the toolbar, click **Save changes**.

12.2.2 Adding a New Profile

- 1 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
- 2 In the toolbar, click your name.
- 3 Click **Configuration Editor** > **Modules** > **Authenticated** > **Update Profile** > **Update Profile Profiles** > **(Edit List)**.
- 4 Click **Add Profile** and specify a name for the profile.
- 5 Click **OK**.
- 6 In **LDAP Search Filter**, specify `(|((objectClass=person)(&((mobile=*)(city=*))(!(homepostaladdress=*))(!(Version=*)))))`.
- 7 In the **Update Profile Form** section, in addition to the contact number and city, add the date of birth and postal address.
- 8 In the toolbar, click **Save changes**.

When filling up the postal address and date of birth details on this form, the user sees the contact number and city that were provided earlier.

12.3 Integrating Profiles with Protected Resources or Custom Portals

The SSPR *New User Registration* module must be publicly accessible whereas the SSPR *Update Profile* module must be protected. To support this, configure URLs as public or restricted by using your proxy or Access Gateway configuration.

You need to integrate the following URLs with a protected resource or a custom portal for which you want to enable progressive profiling:

- ♦ To get the new user registration form: <https://dns-name/sspr/public/newuser>
- ♦ To get the profile: <https://dns-name/sspr/private/updateprofile>

13 Business To Consumer Wizard: Sample Configuration

This section explains how to configure the B2C access management capabilities by using the B2C wizard. This sample configuration is based on the scenario explained in [An Example Scenario](#). This section includes:

- ♦ [Section 13.1, “Prerequisites,” on page 25](#)
- ♦ [Section 13.2, “Using the B2C Wizard,” on page 25](#)

IMPORTANT: This sample configuration and the business to consumer (B2C) wizard are for demonstration purposes only. See [An Example Scenario](#) to deploy B2C capabilities in your environment.

13.1 Prerequisites

- 1 Configure the same user store for Access Manager and Self Service Password Reset. For more information, see “[Configuring Identity User Stores](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*. Ensure that this user store is configured as the default user store. You can view and change the default user store by clicking **Devices > Identity Servers > Edit > Local > Defaults**. Alternatively, you can edit the authentication methods and select this user store.
- 2 Add the Advanced Authentication server certificate and Self Service Password Reset sever certificate to the Identity Server trust store on **Security > Trusted Roots**. For information about adding certificates, see “[Managing Trusted Roots](#)” in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.
- 3 Add the host entries for Access Gateway and Advanced Authentication proxy to all Identity Servers.

13.2 Using the B2C Wizard

- 1 In Administration Console Dashboard, click **Business to Consumer > Configure Access Manager**.
- 2 Specify the following details in **Access Manager Configuration**:

Field	Description
Identity Server Cluster	Select the appropriate Identity Server cluster.
Access Gateway Cluster	Select the appropriate Access Gateway cluster that is associated with the Identity Server cluster that you selected in Identity Server Cluster .

Field	Description
Create Risk-based Policy (optional)	Select to automatically create a risk policy. It also creates an authentication class, a method, and a contract in Identity Server for this policy. NOTE: This risk-based policy creates a device fingerprinting rule. If a device fingerprinting rule already exists, policy will use the existing device fingerprinting rule.
B2C Portal DNS	Specify the B2C Portal DNS or keep the default value. NOTE: B2C Portal DNS Name specified in Access Manager Configuration is updated in Published DNS Name in Self Service Password Reset (SSPR) Server Details and Advanced Authentication Server Details automatically.
B2C Portal IP	Specify the B2C Portal IP address where the <code>index.html</code> and <code>index.css</code> files will be hosted.
Non-Secure Port	Specify a non-secure port value.
Secure Port	Specify a secure port value.

3 Specify the following details in **Self Service Password Reset (SSPR) Server Details**:

Field	Description
Published SSPR URL	Specify the IP address and port number of the Self Service Password Reset server.
API User Name	Specify the secret name that you will specify while configuring the Self Service Password Reset server.
API Password	Specify the secret key that you will specify while configuring the Self Service Password Reset server.

4 Specify the following details in **Advanced Authentication Server Details** (optional):

Field	Description
Configure Advanced Authentication	Select this option if you want to configure Advanced Authentication.
Server Domain	Specify the IP address and the port number of the Advanced Authentication server.
Published DNS Name	Contains the DNS name of the Advanced Authentication server. The default value is <code>aa.b2c.com</code> .

5 Click **OK**.

After the configuration is saved, you will be directed to Configuration Information page.

6 Perform the tasks listed under the **Configuration: Next Steps** pane on the **Configuration Information** page.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

© Copyright 2019 Micro Focus or one of its affiliates.