TECHNICAL INTEGRATION GUIDE

Technical Integration Guide for Entrust Identity AD FS Adapter 13.0

Document issue: 2.0

Date of issue: September 2025

Help us to improve our documentation. Please click this link. and take our survey.

Table of contents

Revision, audience, and guide information

Revisions

Revision	Section	Description
2.0	Configure AD FS for Face Biometric authentication with IDaaS	A new section for Configuring AD FS for Face Biometric authentication with IDaaS has been added.
1.0		The installer has been updated and a new section for setting up Passkey/FIDO2 authentication has been added.

Audience

This guide is intended for organization integrating the Entrust Identity AD FS Adapter solution with Entrust Identity Enterprise (formerly called Entrust IdentityGuard) and Identity as a Service.

Viewing this guide

Although this guide can be printed out, it relies heavily on hyperlinks to other sections. It is best viewed and used electronically.

Introduction

This Technical Integration Guide provides an overview of how to integrate the Entrust Adapter with Microsoft® Active Directory Federation Services (AD FS). The aim of this integration is to add Entrust multi-factor authentication (MFA) to AD FS. The Entrust Adapter uses the pluggable Multi-factor authentication (MFA) option of AD FS to integrate Entrust MFA with AD FS.

Overview

Entrust Identity AD FS Adapter integrates Entrust Identity Enterprise and Identity as a Service (IDaaS) second-factor authentication with Microsoft Active Directory Federation Services.

Entrust Identity Enterprise and Identity as a Service authenticate and manage users and their authentication data. Entrust provides strong second-factor authentication. When AD FS is integrated with the Entrust Identity AD FS Adapter, the Entrust Identity AD FS Adapter serves as a login and re-authentication device to allow for two-factor authentication for system access or to verify certain secured actions.

Integration information

Entrust Product: Entrust Identity Enterprise 13.0 or later and Identity as a Service 5.37 or later

Partner name: Microsoft

Web site: http://www.microsoft.com

Product name: Active Directory Federation Services

Product version: 4.0 and 5.0

Partner Product description: In Windows Server® 2025, Windows Server® 2022, Windows Server® 2016, and Windows Server® 2019, AD FS includes a federation service role service that acts as an identity provider (authenticates users to provide security tokens to applications that trust AD FS) or as a federation provider (consumes tokens from other identity providers and then provides security tokens to applications that trust AD FS). Active Directory Federation Services (AD FS) makes it possible for local users and federated users to use claims-based single sign-on (SSO) to Web sites and services.

AD FS can be used to collaborate securely across Active Directory domains with other external organizations by using identity federation. This reduces the need for duplicate accounts, management of multiple logons, and other credential management issues that can occur when establishing cross-organizational trusts. The AD FS platform provides a fully redesigned Windows-based Federation Service that supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

Authentication overview

The following tables describe the supported authentication methods.

Table 1: Supported authentication methods for Entrust Identity Enterprise

Authentication Type	Description
One-Time Password	In OTP authentication, the user enters a password that can be used only once. In the classic case, the user receives the password only when it is needed.
	Entrust Identity Enterprise allows users to have multiple OTPs. Since OTPs can be used only once, the user's supply of OTPs is reduced with each authentication. When the user's supply of OTPs falls below a threshold, Entrust Identity Enterprise automatically generates and sends a new supply of OTPs.
	The operation and refresh threshold are defined in Entrust Identity Enterprise policy. OTP authentication can be used with a personal verification number (PVN) if your system is set up to require it.
Grid	In grid authentication, the user enters the user ID and password on one page, and the response to the grid challenge on the next page. Grid authentication can be used with a personal verification number (PVN) if your system is set up to require it.
Knowledge Based Q & A	During user registration, the user sets up answers for some predefined (and sometimes user-defined) questions. In knowledge-based authentication, the user answers these previously defined questions.
Token	In token authentication, the user enters a code generated on a hardware or software token in response to a token challenge. Token authentication can be used with a personal verification number (PVN) if your system is set up to require it.
Entrust Soft Token	TVS is a strong out-of-band authentication method where an authentication challenge is sent on user's mobile. This challenge is signed by the Entrust Mobile Soft Token app and verified by Entrust Identity Enterprise server. A user can accept or reject the challenge, which results in either a successful or failed authentication.
Mobile Smart Credentials	Identity Assured is a strong out-of-band authentication method where an authentication challenge is sent on user's mobile. This challenge is signed by the Entrust Mobile smart card app and verified by Entrust Identity Enterprise server. A user can accept, reject, or click suspicious challenge, which results in either a successful or failed authentication.

Authentication Type	Description
Personal Verification Number (Entrust Identity Enterprise only)	Provides an extra level of security when using grids, tokens, and temporary PINs. Any grid, token, or temporary PIN challenge can also include a PVN challenge. By default, no authentication methods require a PVN, so you must set the Entrust Identity Enterprise policy to require PVNs.
	An administrator can create PVNs for your users, or you can let users create and update their own PVNs.
	The PVN can be any length from 1-255 digits, but you should select a length that makes the value easy to remember and enter, while still providing an acceptable level of security. You set the length in the PVN policy on the Entrust Identity Enterprise Server.
	Each user can have just one PVN. You can force a user to update their PVN just after an administrator creates it, or anytime the PVN gets too old. If a user's PVN needs to be changed, the user receives at the next login attempt. The change request appears with the second-factor challenge.
Temporary PIN (Entrust Identity Enterprise only)	A temporary PIN is a fallback authentication method used when the user: • is not yet registered for a grid or token • the user has lost or forgotten their grid or token • The user requests the temporary PIN and receives a password (PIN) that can be used to log on. The temporary PIN can be used to replace grid, or token authentication.
	Temporary PINs can be used with a personal verification number (PVN) if your system is set up to require it.
Machine risk-based authentication	Supports checking the IP address and additional client information (for example persistent browser cookies) of the user logging in.
Passkey/FIDO2	Passkey/FIDO2 authentication can replace the old and traditional way of signing in with fast and secure login experiences. Passkey/FIDO2 specifications have multifactor authentication and public key cryptography. Unlike password authentication, Passkey/FIDO2 stores information, including biometric authentication data, on user devices to prevent it attacks.

Table 2: Supported authentication methods for Identity as a Service

Authentication Type	Description
One-time password (OTP)	In OTP authentication, the user enters a password that can be used only once. In the classic case, the user receives the password only when it is needed by email, SMS, or voice.
	Entrust Identity as a Service Administrators can now create custom attributes to allow users to use alternate email, voice, or SMS delivery options for OTP authentication. When configured, an alternative OTP delivery attribute can be set as the default delivery method. If a user has both a default delivery contact and an alternate delivery contact, the user can click One-Time Password Authentication on the second-factor log in screen and choose another OTP delivery contact.
	The OTP delivery options appear on the user login screen with masked values. For email addresses, the first three characters and the domain name are not masked. For example, `support@entrust.com` appears as `sup***@entrust.com`. For phone numbers, the last 4 digits are not masked. For example, `+12345678910` appears as `******8910`. Note that for short email addresses, the actual address may be visible.
Grid	In grid authentication, the user enters the response to the grid challenge.
Knowledge Based Q & A	During user registration, the user sets up answers for some predefined (and sometimes user-defined) questions. In knowledge-based authentication, the user answers these previously defined questions.
Token	In token authentication, the user enters a code generated on a hardware or software token in response to a token challenge.
Mobile Soft Token	TVS is a strong out-of-band authentication method where an authentication challenge is sent on user's mobile. This challenge is signed by the Entrust Mobile Soft Token app and verified by Identity as a Service. A user can accept or reject the challenge, which results in either a successful or failed authentication.
Mobile Smart Credentials	Identity Assured is a strong out-of-band authentication method where an authentication challenge is sent on user's mobile. This challenge is signed by the Entrust Mobile smart card app and verified by Entrust Identity Enterprise server. A user can accept, reject, or click suspicious challenge, which results in either a successful or failed authentication.
Temporary Access Code	Temporary Access Codes can be used to log in when a user cannot access their one-time passcode (OTP), Grid Card, or token authenticator (for example, if a user has misplaced the mobile device containing their Entrust Soft Token mobile application).
	Note: Temporary Access Codes can also be used as a standalone authenticator rather than as a substitute but Entrust recommends using temporary access codes only for interim authentication."
Machine risk-based authentication	Supports checking the IP address and additional client information (for example persistent browser cookies) of the user logging in.

Authentication Type	Description
Passkey/FIDO2	Passkey/FIDO2 authentication can replace the old and traditional way of signing in with fast and secure login experiences. Passkey/FIDO2 specifications have multifactor authentication and public key cryptography. Unlike password authentication, Passkey/FIDO2 stores information, including biometric authentication data, on user devices to prevent it attacks.
Face Biometric	The Face Biometric authenticator uses Onfido identity verification to verify users. Registration and authentication can be performed using the Entrust Identity Mobile application.

Two-factor authentication

AD FS supports both primary and secondary authentication of users against Active Directory.

Primary authentication

Windows Server 2025, Windows Server 2022, Windows Server 2016, and Windows Server 2019 support the following primary authentication methods:

- Windows integrated authentication
- Username and password
- Client certificate (client Transport Layer Security (TLS), including SmartCard authentication

Secondary authentication

Secondary authentication occurs immediately after primary authentication and authenticates the same Active Directory (AD) user. Once primary authentication is complete and successful, AD FS invokes an external authentication handler. This handler invokes an additional authentication provider, either an in-box AD FS provider or an external MFA provider, based on protocol inputs and policy.

AD FS passes the primary authenticated user's identity to the additional authentication provider, which performs the authentication and returns the results. At this point, AD FS continues executing the authentication/authorization policy and issues the token accordingly.

Authentication flow

AD FS provides extensible Multifactor Authentication by additional authentication providers that are invoked during secondary authentication. AD FS includes, in-box, the x509 certificate authentication provider. Other, external providers developed by AD FS partners can be registered in AD FS by the administrator. Once a provider is registered with AD FS, it is invoked from the AD FS authentication code through specific interfaces and methods that the provider implements and that AD FS calls. Because it provides a bridge from AD FS to the functionality of an external authentication provider, the external authentication provider is also called an *AD FS MFA adapter*.

Figure 1 provides an overview of the AD FS authentication flow using the AD FS Adapter for second-factor authentication with Entrust Identity Enterprise or Identity as a Service.
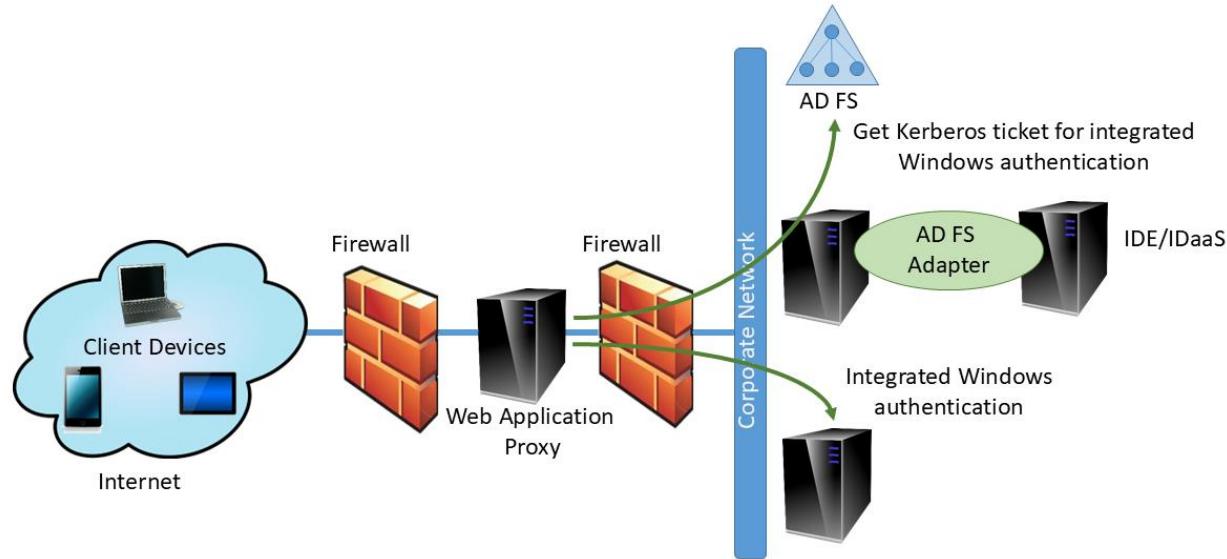
Multifactor authentication flow process

The multifactor authentication flow works as follows:

1. The user accesses a resource protected using AD FS on WAP, for example, Microsoft OWA.

2. The user is redirected to the AD FS primary authentication login page, for example, forms authentication or Integrated Windows Authentication (IWA).

3. AD FS performs the primary authentication by validating the credentials with Active Directory Domain Service.

4. AD FS invokes the Entrust Identity AD FS Multifactor Authentication Adapter.

5. Entrust Identity AD FS Adapter submits the second-factor challenge page to AD FS and then presents it to the user.

6. The user provides SF response to Entrust Identity AD FS Adapter by way of AD FS.

7. Entrust Identity AD FS Adapter verifies second-factor response and returns success or failure to AD FS.

8. AD FS issues a security token (WS-trust, WS federation or SAML 2.0) and redirects to original protected resource.

Performing the integration

To integrate Active Directory Federation Services and the Entrust Identity AD FS Adapter complete the following steps:

Integrate with Entrust Identity Enterprise

To integrate with Entrust Identity Enterprise

1. Install and configure AD FS.

2. Install and configure WAP.

3. Publish an AD FS sample application on WAP.

4. Install Entrust Identity AD FS Adapter.

5. Restart the AD FS service.

6. Configure AD FS for Entrust authentication.

7. Test the integration by publishing a WAP application.

Note: This guide assumes that you have WAP, AD FS 4.0 or 5.0 and at least one Relying Party, protected by AD FS working prior to Entrust Identity AD FS Adapter integration. Appendix A provides instructions on installing and configuring AD FS, WAP, and a publishing application. However, it is expected that customers contact Microsoft support if they encounter any issues.

Integrate with Identity as a Service

To integrate with IDaaS

1. Add AD FS as an authentication API to IDaaS.

2. Create a resource rule in IDaaS to protect access to AD FS.

3. Install and configure AD FS 5.0.

4. Restart the AD FS service.

5. Configure AD FS for Entrust authentication.

6. Configure AD FS for Soft Token Push with Mutual Auth challenge.

7. Test integration by publishing a WAP application.

Installing Entrust Identity AD FS for IDaaS

If you want to install Entrust Identity AD FS installer for Identity as a Service, you must:

1. Add Authentication API to IDaaS and copy the Application ID for use in the Entrust Identity AD FS Adapter installer.

2. You must also create a resource rule to protect your resource.

See Integrate AD FS Adapter in the *Technical Integrations Guides* for more information.

Prerequisites

.Net framework 4.8 must be installed.

Installing the Entrust Identity AD FS Adapter

The following instructions provide details on installing Entrust Identity AD FS Adapter.

This section includes the following topics:

- [Prerequisites](#)
- [Adding an Authentication API to Identity as a Service](#)
- [Install the Entrust Identity AD FS Adapter primary server](#)

Prerequisites

Before you begin the installation, ensure that the following prerequisites are met:

- You must install the Entrust Identity AD FS Adapter Plugin installer on the primary AD FS Server first and then later on the secondary AD FS Server Farm.
- Microsoft Services Active Directory Federation Services should be in a Running state during the installation of the Entrust Identity AD FS Adapter Plugin installer.
- If you are installing on IDaaS, you must first add an Authentication API to Identity as a Service to generate an Application ID. You need to add the Application ID during the Entrust Identity AD FS Adapter installation. You also need to create a resource rule in IDaaS for Entrust Identity AD FS.

Install the Entrust Identity AD FS Adapter primary server

Choose from the following procedures:

- [Install Entrust Identity AD FS Adapter for Entrust Identity Enterprise](#)
- [Install the Entrust Identity AD FS Adapter for Identity as Service](#)

Install Entrust Identity AD FS Adapter for Entrust Identity Enterprise

To install the Entrust Identity AD FS Adapter for Entrust Identity Enterprise

1. Download the Entrust Identity AD FS Adapter software from Entrust Trusted Care at https://trustedcare.entrust.com.
2. Copy the software to your computer.
3. Double-click the `IDE_ADFS_Adapter_13.0.msi` installer file. The **Entrust Identity AD FS Adapter Setup Wizard** appears.

4. Click **Next** to continue.

5. Click **Next** to begin the installation. The **License Agreement** page appears.

6. Read the license agreement for Entrust Identity software carefully, and select **I accept the license agreement**.

7. Click Next. The Federation Server Setup page appears.

8. On **the Federation Server setup** page, select one of the following options:

- Select **Primary ADFS server** if you are installing on a primary server.
- Select **Other ADFS server** if you are installing on another AD FS server.

9. Click Next. The Authentication Server Setup page appears.

10. Select Entrust Identity Enterprise Server.

11. Click **Next**. The **Authentication Adapter Setup** page appears.
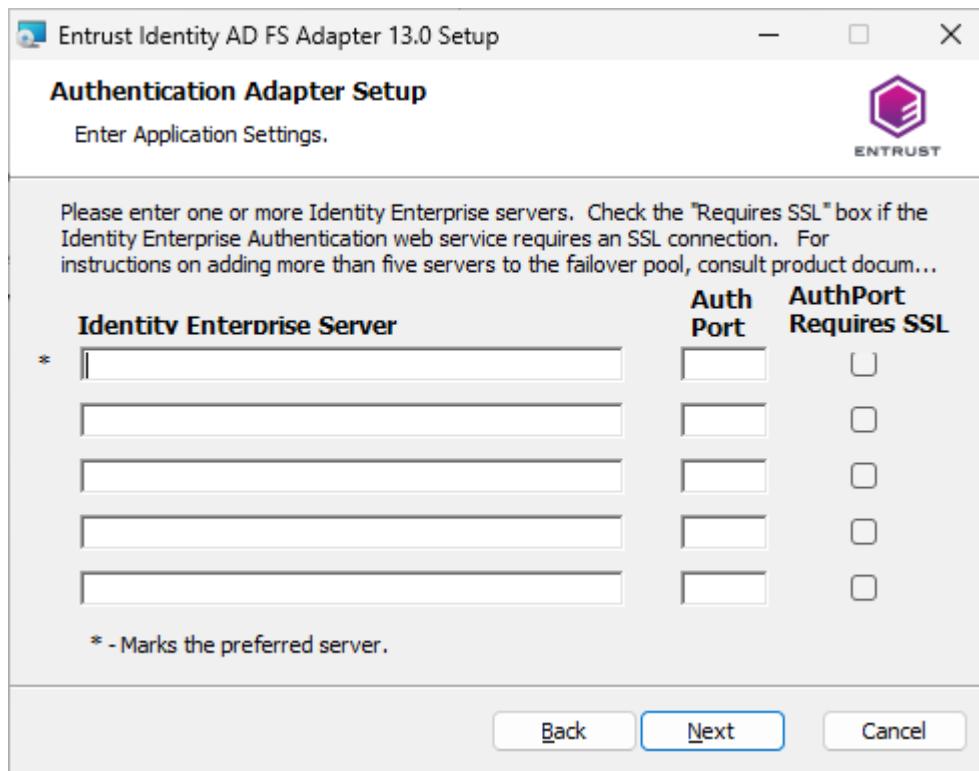
12. In the **Authentication Adapter Setup** page, do the following:

a. Enter the host names of one or more Entrust Identity Enterprise servers in the **Identity Enterprise Server** fields.

If you need to configure more than five Entrust Identity Enterprise Servers, you can add the extra servers after installation is complete. See "*Appendix B: Configuring failover for Entrust Identity Enterprise Servers.*"

Note: The preferred Entrust Identity Enterprise Server (number 1) is the Primary Entrust Identity Enterprise Server in a high availability failover scenario.

b. Enter the port number being used by the Entrust Identity Enterprise authentication service in the **Auth Port** field.

Default port assignment numbers:

```
8080   non-SSL
8443   SSL
```

c. If needed, select Auth Port Requires SSL.

Note: If you select SSL, you must already have imported the appropriate certificates into the local computer store of the computer where you are installing the Entrust Identity AD FS Adapter.

13. Click Next. The Authentication Provider Setup page appears.
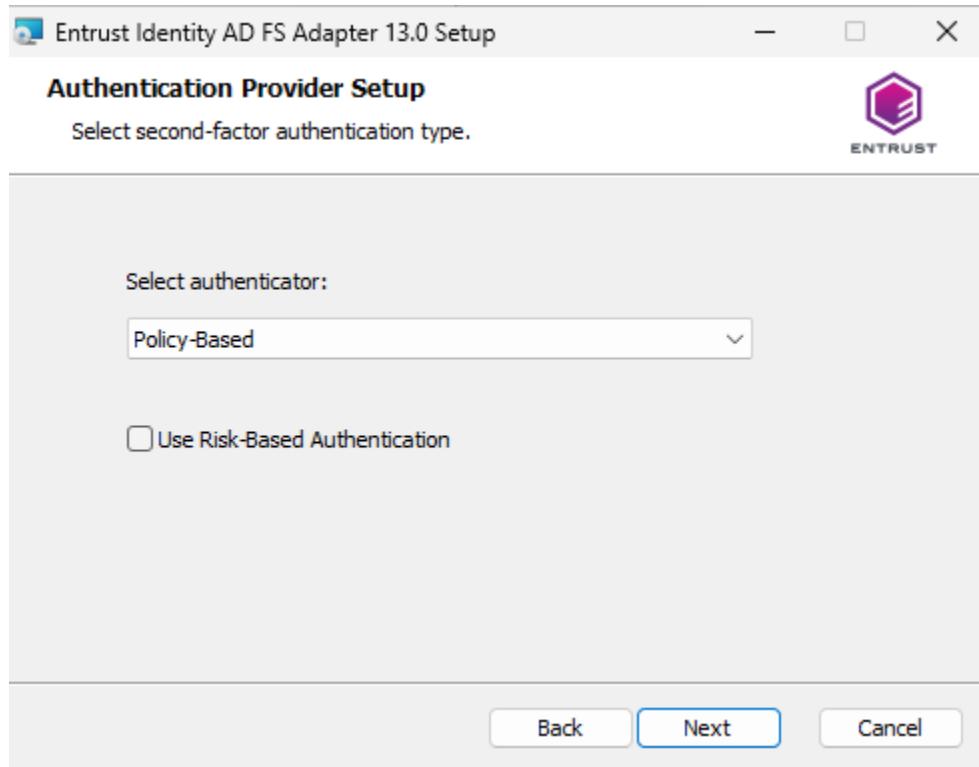
14. In the Authentication Provider Setup page, do the following:

a. Select the second-factor authenticator type from the drop-down list. The default is **Policy-based**.

b. Optionally, select **Use Risk-Based Authentication** if you want to enable machine authentication.

15. Click **Next**.

Note: If you selected **Policy-based** authenticator in the previous step, the **Paskey Configuration Setup** page appears.

Entrust Identity AD FS Adapter 13.0 Setup

Passkey Configuration Setup

Enter Passkey configuration settings.

Relying Party ID (cluster name) :

Make sure this value matches the registered 'Passkey Relying Party ID' value.

☑ Allow Origin SubDomain

Enabling 'Allow Origin SubDomain' will allow a match to any host in the above domain and any sub domains it may include

☐ Allow Origin Port

Enable 'Allow Origin Port' if an app authentication taking place is not running on the default TLS port (i.e., 443)

[Back] [Next] [Cancel]

16. In the **Passkey Configuration Setup** page, do the following:

   a. In the **Relying Party ID (cluster name**) field, enter the Relying Party ID that users have used to register the Passkey. It can be a qualified domain name (FQDN) or the domain itself. The following provides an example of valid Relying Party ID values:

      `<cluster name>.<subdomain>.<domain.com>.`

      `<subdomain>.<domain.com>`

      `<domain.com>`

      This property must be set for the following:

      – If you are enabling passkey authentication to Entrust Identity Self-Service Module.

      –or–

      – If you are enabling the self-administration action that allows a passkey to be registered.

   b. Select **Allow Origin Subdomain** to require the origin returned by the passkey to match the allowed origin associated with the Entrust Identity Enterprise relying party.

      If the allowed origin references a host name, then successful passkey registration and authentication can only take place using apps running on that host.

      Note: Entrust recommends that passkey registration takes place from any host where Entrust Identity Self-Service Module is installed, and that passkey authentication takes from any host that is running an app that requires Entrust Identity Enterprise to access protected resources. This setup requires the allowed origin to reference a domain (for example, `mycompany.com`) and the property must be set to true (the default is `false`) to allow a match to any host in that domain and any subdomains it may include.

   c. Select **Allow Origin Port** if the app users will use for passkey registration or authentication is not running on the default TLS port (for example, 443). The default is `true`.

You cannot associate a port number with the relying party ID (see https://www.w3.org/TR/webauthn-2/#rp-id), if the client origin returned by a passkey includes a port number. As a result, it is necessary to relax the origin matching rule so that any port is allowed.

By default, Entrust Identity Self-Service Module is configured to run on port 8445. If you use a reverse proxy to expose your Entrust Identity Self-Service Module instances on port 443, and all applications that require Entrust Identity Enterprise passkey authentication are also accessible through port 443, set this property to `false`.

17. Click **Next**. The **Cookie Domain** page appears.
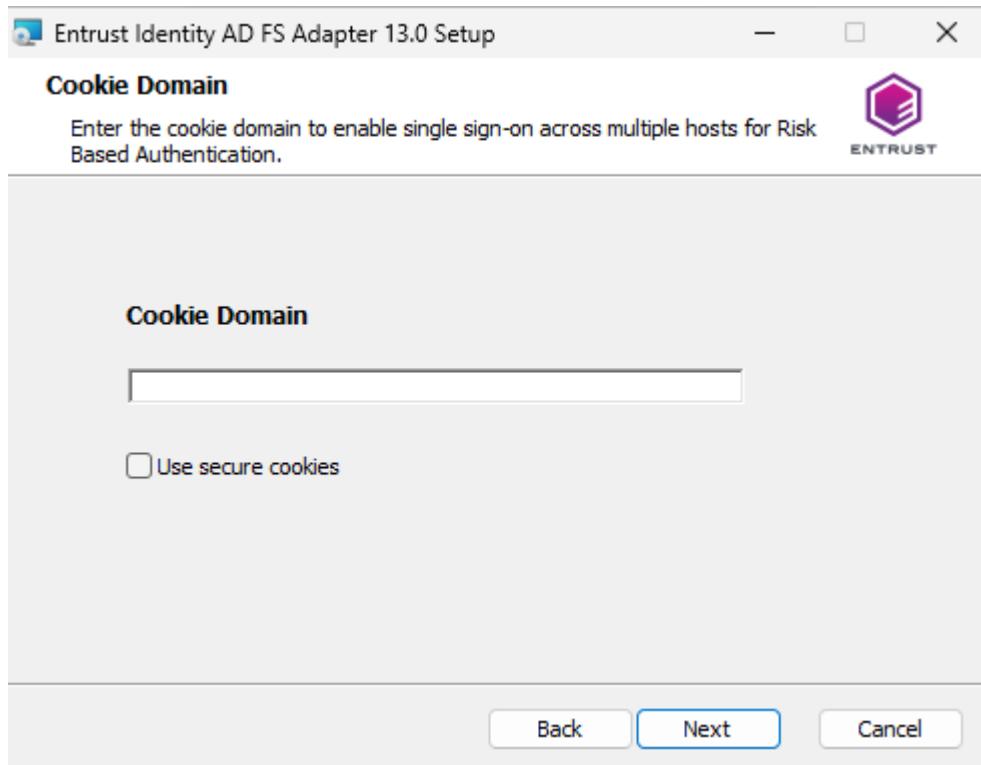
18. If you are using risk-based authentication, provide the cookie domain for Entrust Identity Enterprise authentication cookies.

Note: This step is optional if you are not using risk-based authentication.

19. Click **Next**. The **Destination Folder** page appears.
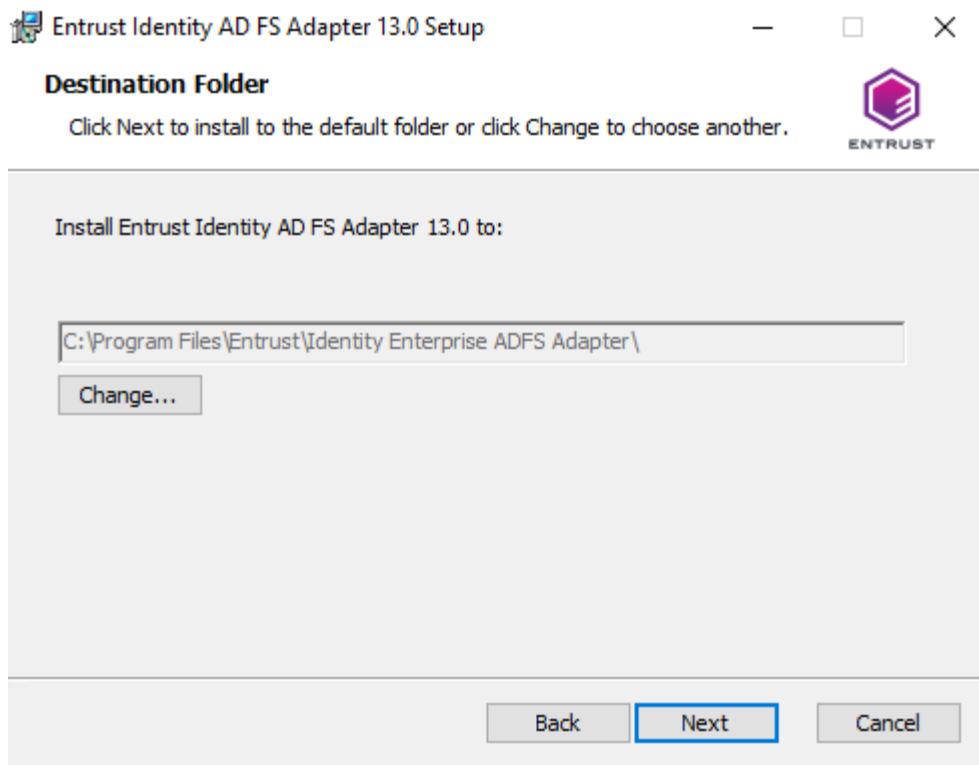
20. Select the folder where you want to install the application and click **Next**.

21. The Ready to Install Entrust Identity AD FS Adapter page appears.
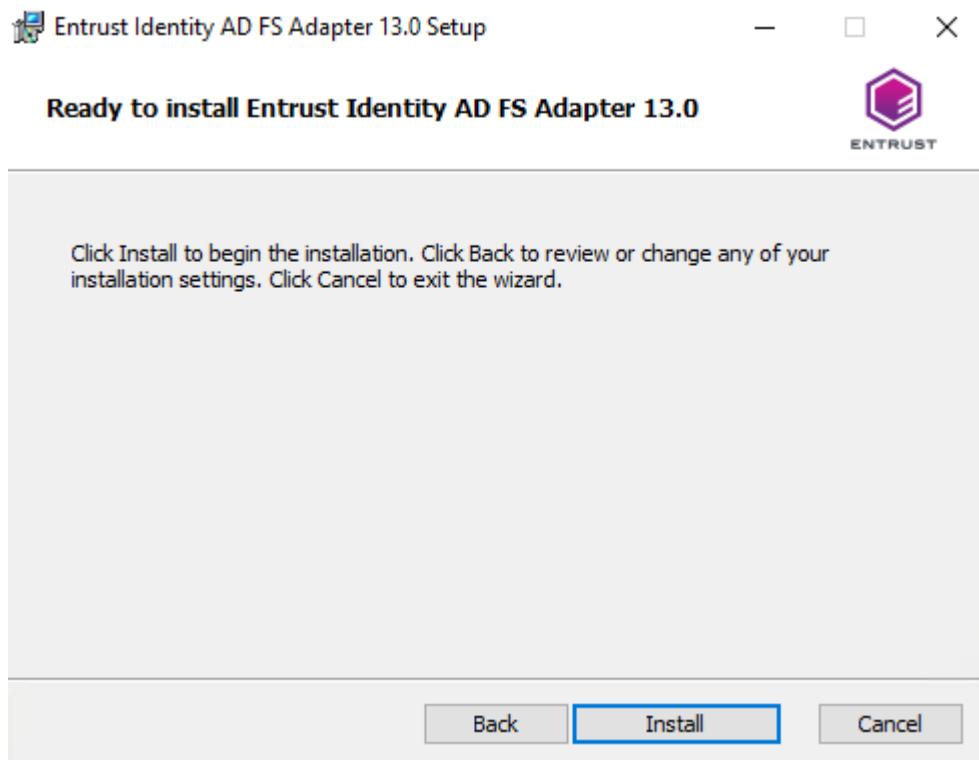
22. Click **Install** to start the installation.

23. The Completed Entrust Identity AD FS Adapter Setup Wizard page appears.

24. Click **Finish** to exit the Setup Wizard. You must now restart your AD FS service.

Install the Entrust Identity AD FS Adapter for Identity as Service

To install the Entrust Identity AD FS Adapter for Identity as a Service

1. Download the Entrust Identity AD FS Adapter software from Entrust Trusted Care at https://trustedcare.entrust.com.

2. Copy the software to your computer.

3. Double-click the `IDE_ADFS_Adapter_13.0.msi` installer file. The **Entrust Identity AD FS Adapter Setup Wizard** appears.

4. Click **Next** to continue.

5. Click **Next** to begin the installation. The **License Agreement** page appears.

6. Read the license agreement for Entrust Identity software carefully, and select **I accept the license agreement**.

7. Click Next. The Federation Server Setup page appears.

8. On **the Federation Server setup** page, select one of the following options:

- Select **Primary ADFS server** if you are installing on a primary server.
- Select **Other ADFS server** if you are installing on another AD FS server.

9. Click Next. The Authentication Server Setup page appears.

10. Select Entrust Identity as a Service (IDaaS).
11. Click **Next**. The **Authentication Adapter Setup** page appears.

Entrust Identity AD FS Adapter 13.0 Setup

Identity as a Service Authentication Setup

Enter Identity as a Service Application Settings.

Identity as a Service Tenant URL :

https://

Example: <customer>.<region>.trustedauth.com

Identity as a Service Application ID :

This Application ID is displayed by Identity as a Service after creating an Authentication API application in the Identity as a Service Administration Portal.

[Back] [Next] [Cancel]

a. In the **Identity as a Service Tenant URL** field, enter the Identity as a Service Tenant URL. For example,

   <my_company>.<region>.trustedauthdev.com

b. In the **Identity as s Service Application ID** field, enter **the Application ID** that what generated when you created the Authentication API in Identity as a Service (See Integrate AD FS Adapter in the Identity as a Service Integration Guides for more information.)

12. Click Next. The Authentication Provider Setup page appears.

13. Click Next. The Paskey Configuration Setup page appears.
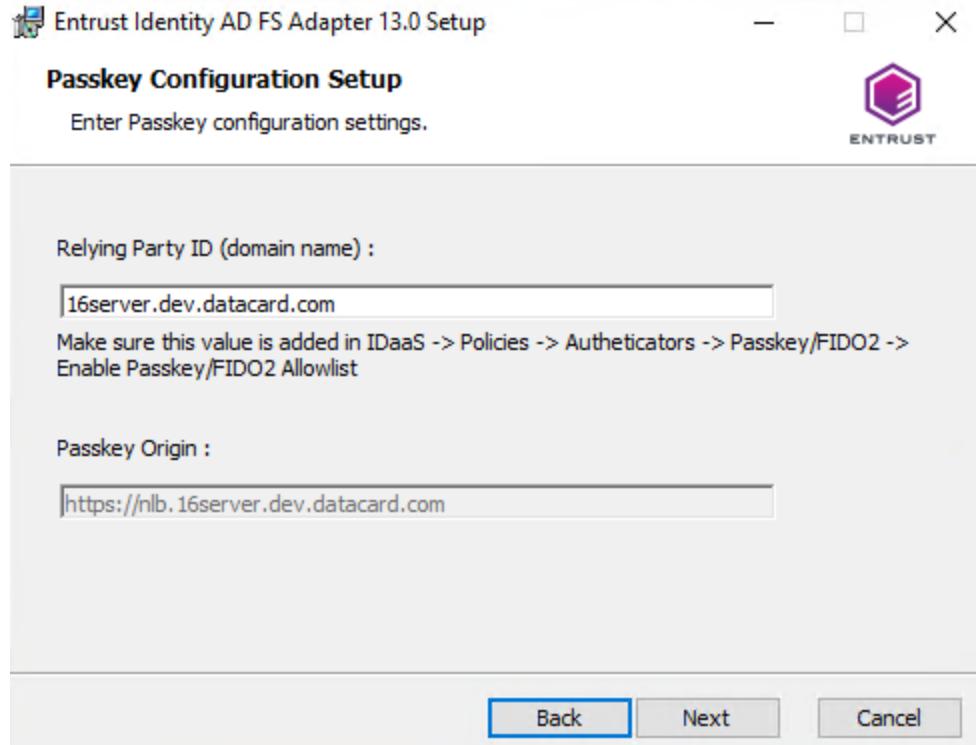
14. In the **Passkey Configuration Setup** page, do the following:

   a. In the **Relying Party ID (cluster name**) field, enter the Relying Party ID that the users have used to register the Passkey. It can be a qualified domain name (FQDN) or the domain itself. The following provides an example of valid Relying Party ID values:

   ```
   <cluster name>.<subdomain>.<domain.com>.
   ```

   ```
   <subdomain>.<domain.com>
   ```

   ```
   <domain.com>
   ```

   This property must be set for the following:

Note: You must add **Relying Party ID** value to the **Passkey/FIDO2 Allowlist** in IDaaS. See Modify Passkey/FIDO2 authenticators in the *IDaaS Administrator help*.

   b. The **Passkey Origin** is populated by default.

15. Click **Next**. The **Cookie Domain** page appears.
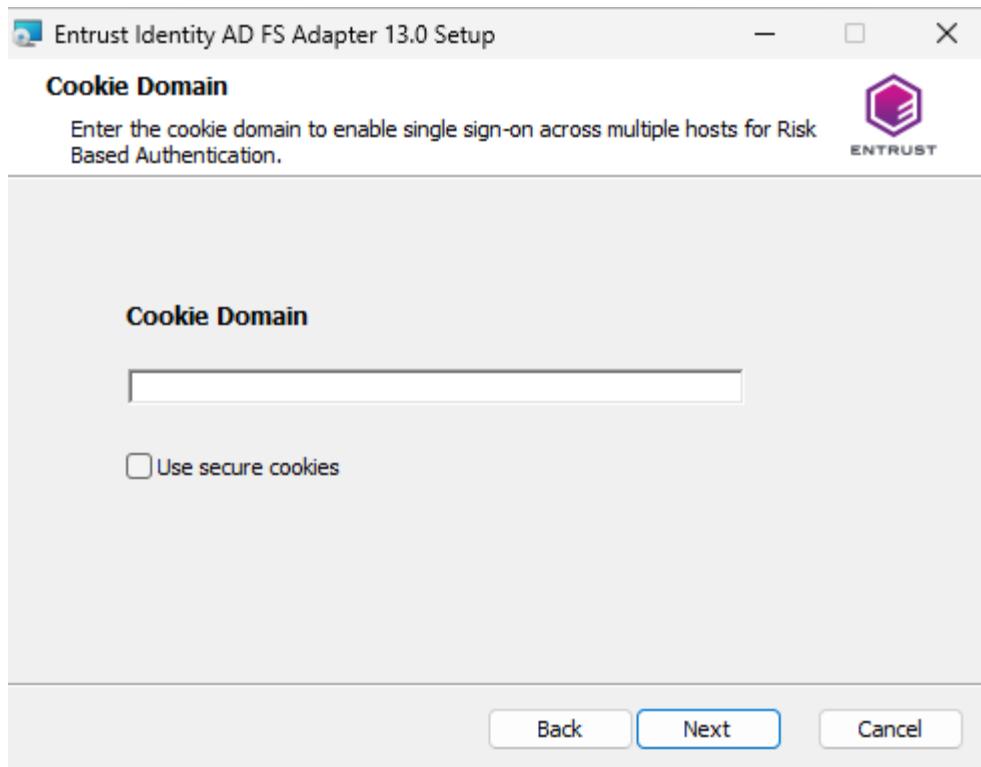
16. If you are using risk-based authentication, provide the cookie domain for IDaaS authentication cookies.

**Note:** This step is optional if you are not using risk-based authentication.

17. Click **Next**. The **Destination Folder** page appears.
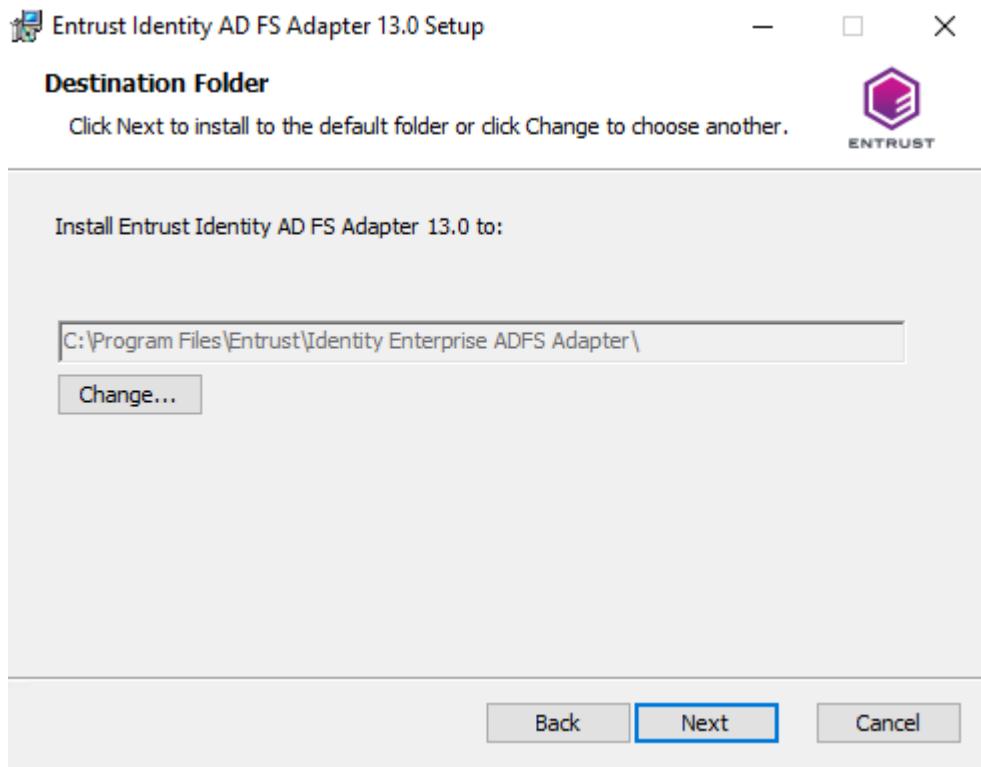
18. Select the folder where you want to install the application and click **Next**.

**19.** The Ready to Install Entrust Identity AD FS Adapter page appears.
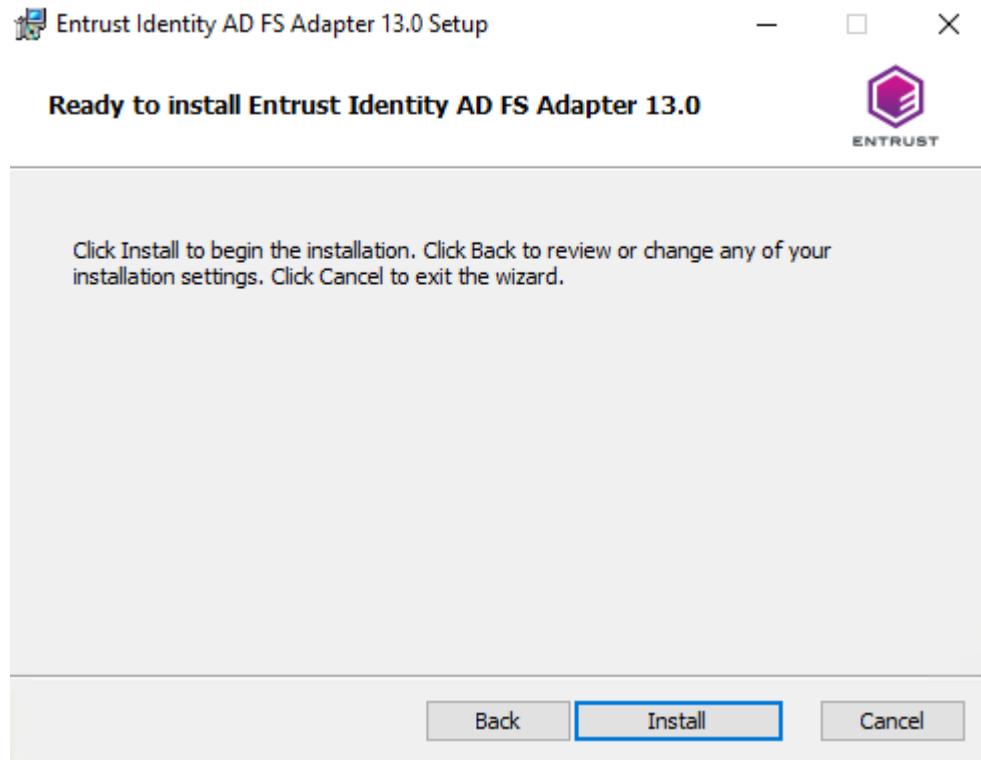
20. Click **Install** to start the installation.

21. The Completed Entrust Identity AD FS Adapter Setup Wizard page appears.

22. Click **Finish** to exit the Setup Wizard. You must now restart your AD FS service.

Restarting the AD FS service

To restart the AD FS service

1. Go to Control Panel > System and Security > Administrative Tools > Services to display your list of services.

2. Right-click **Active Directory Federation Services** and select **Restart** from the drop-down menu.

Configuring AD FS for Entrust authentication

To configure AD FS for Entrust authentication you must create the AD FS policy that invokes the Entrust Identity AD FS Adapter.

To configure AD FS 13.0 for Entrust Authentication

1. Ensure that you have restarted the Active Directory Federation Services after installing the Entrust Identity AD FS Adapter (see Restarting the AD FS service).

2. Go to **Start > Administrative Tools** and double-click **AD FS Management** to open the AD FS Console. The **AD FS Console window** appears.

3. Click Service >>**Authentication Methods**. The AD FS Authentication Methods Overview page appears.
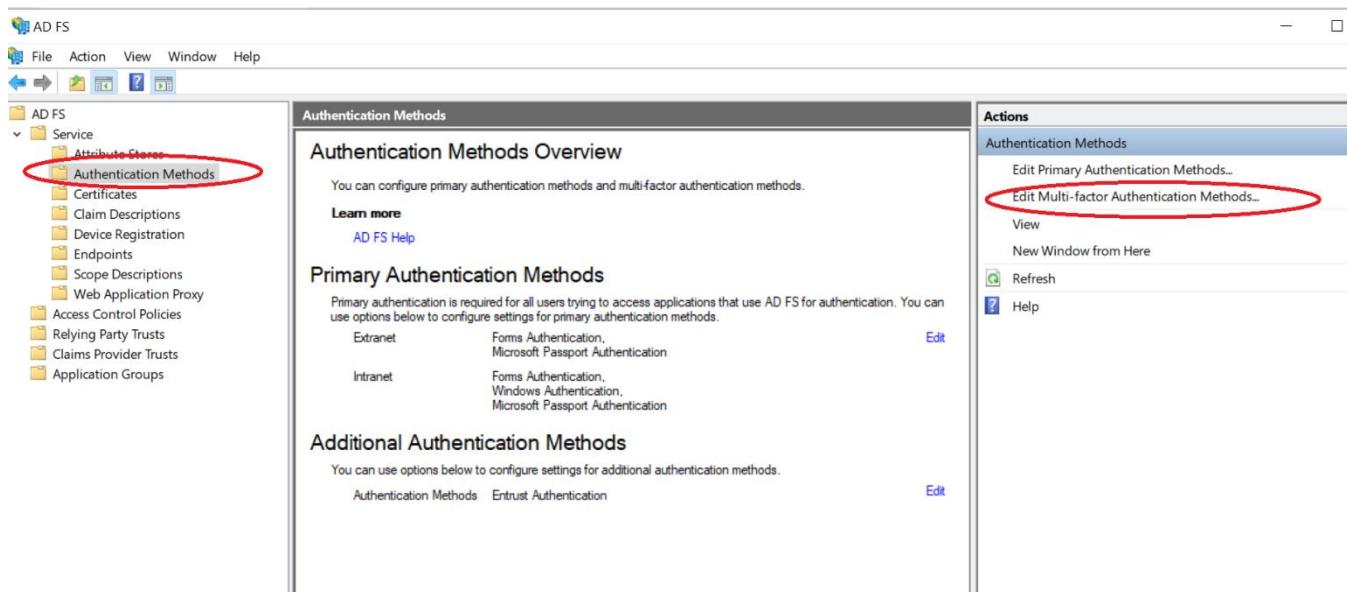
4. Click **Edit Multi-factor Authentication**. The Edit Policy Authentication page appears.
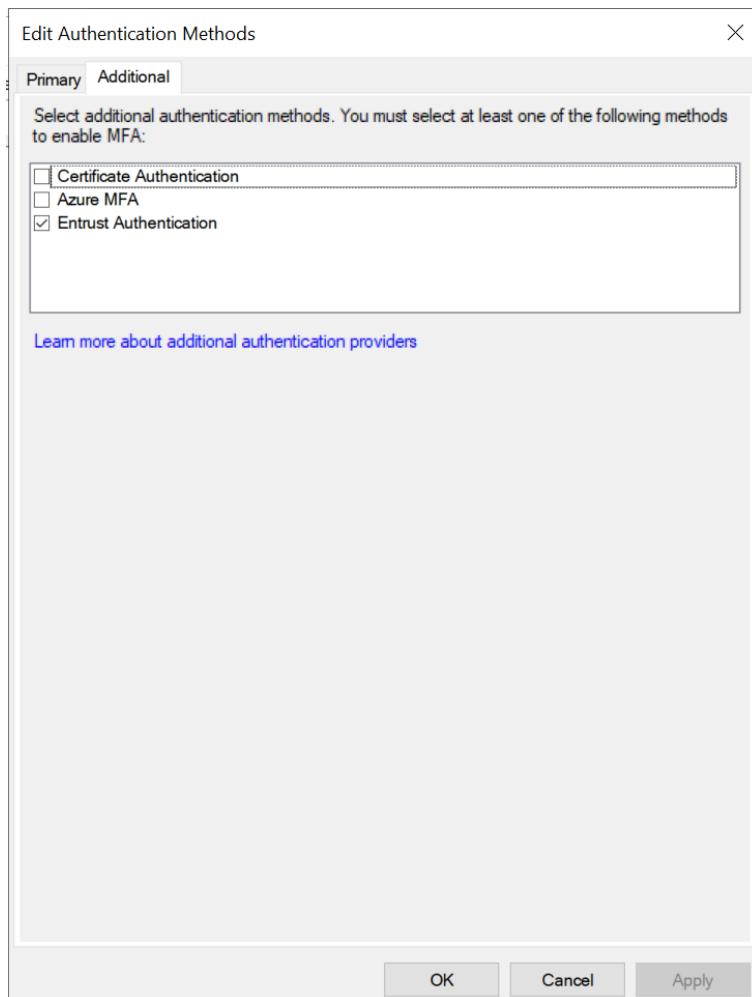
5. Check **Entrust Authentication** to invoke Multi-factor authentication using the Entrust Identity AD FS Adapter.

6. Optional selections:

    a. Under **Users/Groups**, click **Add** to add users or groups that require MFA using the Entrust Identity AD FS Adapter

    b. Under **Devices**, select **Unregistered Devices**, **Registered Devices**, or both as the triggers to invoke MFA using the Entrust Identity AD FS Adapter.

    c. Under **Locations**, select **Extranet**, **Intranet** or both as the triggers to invoke MFA using the Entrust Identity AD FS Adapter.

7. Click **OK**.

Configure AD FS for soft token push with mutual authentication challenge

Mutual authentication challenge requires users to respond to a mutual push authentication challenge. When enabled, users must match the challenge that appears on the IDaaS page with the mutual challenge shown in their Entrust Identity soft token app.

This procedure assumes that you have already integrated AD FS with IDaaS. See the *Identity as a Service Technical Integration Guides* online help for assistance.

Complete these steps:

- Configure soft token push for mutual authentication
- Change the AD FS resource rule in IDaaS
- How mutual authentication works

Configure soft token push for mutual authentication

1. Log in to Identity as a Service.
2. Go to **Home > Policies > Authenticators**.
3. Select **Entrust Soft Token**. The **Entrust Soft Token** page appears.
4. Select **Enable Mutual Challenge**.
5. Click **Save**.

> **Enable Mutual Challenge**
>
> ☑ A flag indicating whether mutual challenge is enabled. Once enabled, the user will be prompted for mu
>
> **Mutual Challenge Size ***
> The number of mutual challenges sent in a transaction.
>
> 4
>
> **Mutual Challenge Length ***
> The number of characters in a mutual challenge.
>
> 4
>
> **Mutual Challenge Alphabet ***
> The characters that can appear in a mutual challenge.
>
> 0123456789
>
> **Mutual Challenge for Percent of Requests ***
> The percentage of requests that will have a mutual challenge.
>
> 100

See Modify Entrust ST authenticators settings in the *IDaaS Administrator Help* for more information.

Change the AD FS resource rule in IDaaS

1. In IDaaS, go to **Home > Security > Authentication Flow**.
2. Create a custom authentication flow with the following settings:

- **User Login** for the login flow

- **External Authentication** for first-factor

- **Entrust Soft Token Push** for second-factor

See Create authentication flows in the IDaaS administrator Help for more information.

3. Create a resource rule for AD FS that uses the custom authentication flow you created in the previous step. See IDaaS applications resource rules in the IDaaS *Administrator* Help for more information.

How mutual authentication works

1. Access the AD FS resource and enter your username and password in first factor page.

2. In second-factor page, the mutual auth push token challenge number appears as shown below.
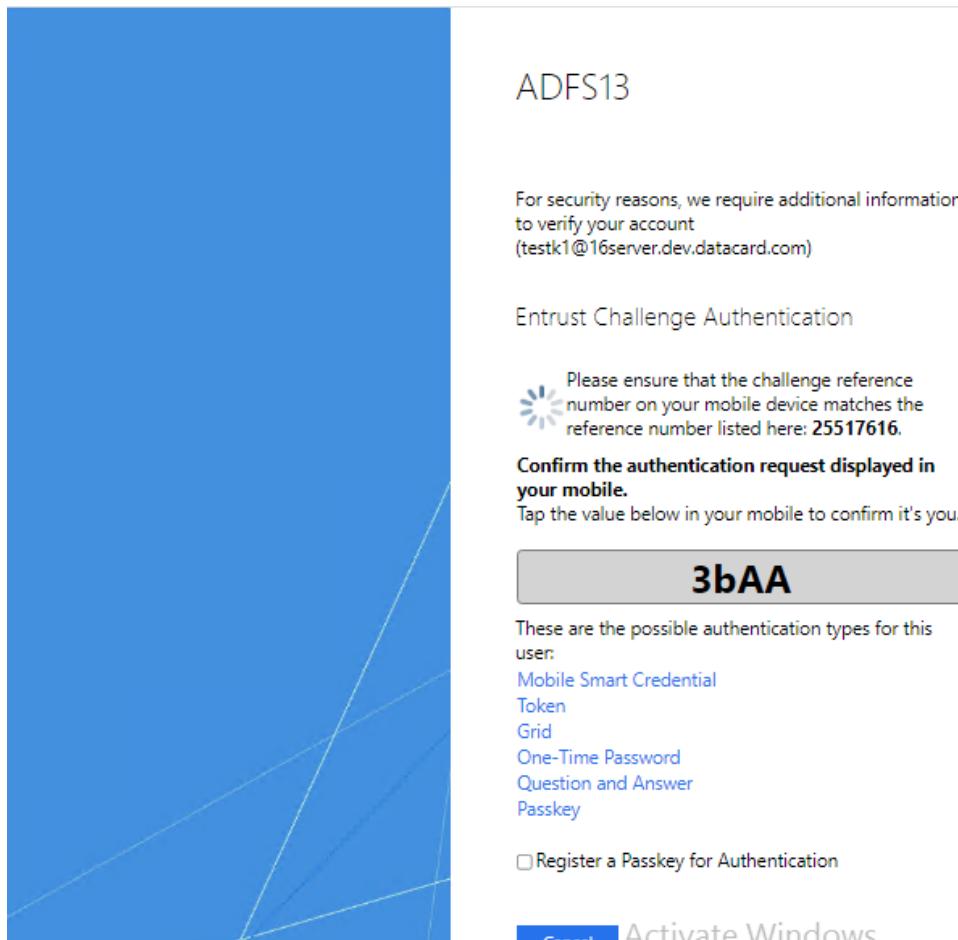
3. The user receives the notification in their mobile device in an Entrust Identity app.

4. The user clicks the notification message to see more about the request and then clicks **Confirm**.

5. The user clicks the value that appears on the resource second-factor authentication page.

← **Confirm the Value**

Select the value that matches the one displayed
where you initiated the transaction.

This is an extra step to protect your account and
confirm your identity. If you do not recognize the
transaction, go back and tap Suspicious. The
transaction will be cancelled.

Bb2A   3bAA   333b

6. The user is redirected to the resource page on successful authentication.

Configure AD FS for Passkey/FIDO2 authentication with IDaaS

Passkey/FIDO2 authentication requires users to respond to the notification sent to their mobile device or passkey token. The user must match the relying party ID on the IDaaS page with the AD FS configuration file.

Note: This procedure assumes that you have already integrated AD FS with IDaaS. See Integrate AD FS Adapter in the *Technical Integrations Guides* for more information.

To configure AD FS for Paskey/FIDO2 with IDaaS

1. Configure Passkey/FIDO2 for multifactor authentication. See Modify Passkey/FIDO2 authenticator settings in the IDaaS *Administrator Help*.

   - Select **Enable Passkey/FIDO2 Allowlist** and include the **Relying Party ID** you configured when you installed the AD FS Adapter for Identity as a Service. See Modify Passkey/FIDO2 authenticator settings in the IDaaS *Administrator Help*.

2. Create a custom user login **Authentication Flow** to enable Passkey/FIDO2 for second-factor authentication. See Create authentication flows in the *IDaaS Administrator Help*.

3. Create a resource rule that includes the Authentication Flow that enables PasskeyFIDO2 for second-factor authentication. See Create a resource rule in the IDaaS *Administrator help*.

4. To enable Passkey Registration option(Register a Passkey for Authentication checkbox), go to <adfs_adapter_install>\IDaaS ADFS Adapter\config and open the eigadfsplugin.xml file and then add <ShowPasskeyRegistrationOption>true</ShowPasskeyRegistrationOption> after <AllowOriginPort>. Save the file and restart the AD FS service.

   (By default this option is not visible.)

How to use Passkey/FIDO2 for registration and authentication

The following sections describe how to register a Passkey/FIDO2 authenticator and then use Passkey/FIDO2 for authentication.

Topics in this section:

- Register a Passkey/FIDO2 token
- Authenticate using a Passkey/FIDO2 token
- Register a Passkey/FIDO2 authenticator with a mobile device
- Authenticate using Passkey/FIDO2 with a mobile device

Register a Passkey/FIDO2 token

To register a Passkey/FIDO2 token

1. Before you begin, locate your Passkey/FIDO2 token that is compliant with compliant with the FIDO2/WebAuthn specification.

2. Access the AD FS resource and enter your username and password in first-factor page.

3. In second-factor page, answer the challenge and select the **Register a Passkey for Authentication** checkbox.

ADFS13

For security reasons, we require additional information
to verify your account
(gajarea@16server.dev.datacard.com)

Entrust Challenge Authentication

To establish your identity, please respond to the
following:

Enter a response to the grid challenge [D4] [H3] [H4]
using a card with serial number: 45

| . | | . | | . |

These are the possible authentication types for this
user:
Mobile Smart Credential
Mobile Soft Token
Token
One-Time Password
Question and Answer

☑ Register a Passkey for Authentication

Submit

4. Click **Submit**. You are prompted to enter the **Passkey Name**.

ADFS13

For security reasons, we require additional information
to verify your account
(gajarea@16server.dev.datacard.com)

Register a Passkey for Authentication

To register a passkey for authentication, enter a name
for your passkey and select the Register button below.

Passkey Name

[   ]

[Register] [Cancel]

⬡ ENTRUST

5. Enter the **Passkey Name** and then click **Register**.

6. Follow the screen prompts to complete Passkey/FIDO2 registration.

Authenticate using a Passkey/FIDO2 token

To authenticate using Passkey/FIDO2 a token

1. Before you begin, locate your Passkey/FIDO2 token that is compliant with compliant with the FIDO2/WebAuthn specification.

2. Clear all browser cookies.

3. Access the AD FS resource and enter your username and password.

4. In the **Challenge Authentication** page, click **Passkey**.

ADFS13

For security reasons, we require additional information
to verify your account
(........)

Entrust Challenge Authentication

To establish your identity, please respond to the
following:

Enter a response to the grid challenge [A3] [B1] [J4]
using a card with serial number: 45

These are the possible authentication types for this
user:
Mobile Smart Credential
Passkey
Mobile Soft Token
Token
One-Time Password
Question and Answer

☐ Register a Passkey for Authentication

Submit

☐ Remember me on this device

ENTRUST

5.   A **Remember me on this device** pop-up appears.

server.mycompany.com   says

Would you like to enable "Remember me on this device" option?

OK   Cancel

6.   To enable RBA, click **OK**. If you do not want to enable RBA, click **Cancel**.

7.   Follow the screen prompts to complete Passkey/FIDO2 authentication.

To register a Passkey/FIDO2 authenticator with a mobile device

1. Clear all web browser cookies.

2. Go to the AD FS resource and enter your username and password in first-factor page. The second-factor page appears.

3. In the second-factor page answer the challenge and then select **Register a Passkey for Authentication**. The **Sign-in with your passkey** page appears.

ADFS13

For security reasons, we require additional information
to verify your account
(gajarea@16server.dev.datacard.com)

Register a Passkey for Authentication
To register a passkey for authentication, enter a name
for your passkey and select the Register button below.

Passkey Name

[   ]

[Register] [Cancel]

ENTRUST

4. Enter the **Passkey Name** and click **Register**. The **Sign in with your passkey** page appears.

5. Select **iPhone, iPad, or Android device** and click **Next**.

6. Scan the QR code of the mobile device.

7. Follow the screen prompts on the device to complete Passkey/FIDO2 registration.

Authenticate using Passkey/FIDO2 with a mobile device

To authenticate using Passkey/FIDO2 with a mobile device

1. Clear all web browser cookies.

2. Go to the AD FS resource and enter your username and password in first-factor page. The second-factor page appears.

ADFS13

For security reasons, we require additional information
to verify your account
(gi_____)

Entrust Challenge Authentication

To establish your identity, please respond to the
following:

Enter a response to the grid challenge [A3] [B1] [J4]
using a card with serial number: 45

These are the possible authentication types for this
user:
Mobile Smart Credential
Passkey
Mobile Soft Token
Token
One-Time Password
Question and Answer

☐ Register a Passkey for Authentication

Submit

3. In the second-factor page, select **Passkey**. The **Sign-in with your passkey** page appears.
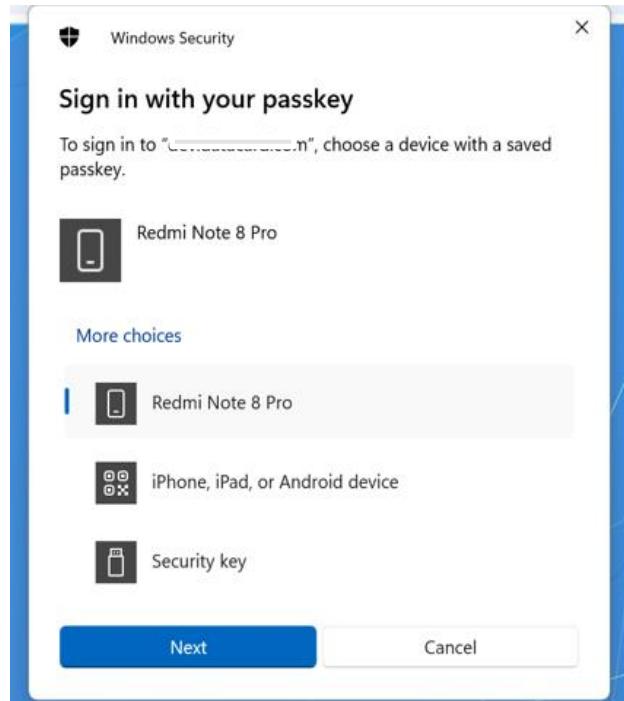
🛡 Windows Security   ✕

Sign in with your passkey

To sign in to "L_____.n", choose a device with a saved
passkey.

📱 Redmi Note 8 Pro

More choices

📱 Redmi Note 8 Pro

📷 iPhone, iPad, or Android device

🔑 Security key

| Next | Cancel |

ADFS13

For security reasons, we require additional information
to verify your account
(_____

To establish your identity, please respond to
the following:

Complete the Passkey Challenge Response

These are the possible authentication types for this
user:
Grid
OTP Authentication using Email

☑ Remember me on this device

4. Select the registered device and click **Next**.

5. The user receives the notification on their mobile device.

6. After successful authentication, the user is logged into the protected resource.

Configure AD FS for Passkey/FIDO2 with Entrust Identity Enterprise

Passkey/FIDO2 authentication requires users to respond to the notification they receive on their mobile device or token. The Relying party ID must be set for the following:

- You are enabling passkey authentication to Entrust Identity Self-Service Module.

–or–

- You are enabling the self-administration action that allows a passkey to be registered.

The relying party is associated with an origin (the allowed origin), which is either a single host or any host that belongs to a domain or associated subdomains.

You need to complete the following procedures using documentation available on Entrust Trusted Care:

- Configure Passkey/FIDO2 for multifactor authentication
- Register Passkey/FIDO2 token with Entrust Identity Self-Service Module

You need to log in to your Trusted Care account to access the documentation to help you complete these procedures.

To access the documentation on Trusted Care

1. Go to https://trustedcare.entrust.com and enter your username and password.
2. Click Products.
3. Scroll to Entrust Enterprise.

Configure Passkey/FIDO2 for multifactor authentication

1. In TrustedCare, go to Products > Entrust Enterprise > Self-Service Module.
2. Click the **Documents** tab.
3. Click to **View** to open the *Entrust Identity Self-Service Module Installation and Configuration Guide*.
4. In the table of contents, go to **Properties > FIDO2 Passkey Configuration**.
5. Follow the procedure in the section "FIDO2 Passkey Configuration" to configure Passkey/FIDO2 for multifactor authentication.

Note: In the **Passkey Relying Party ID** field, enter the Relying Party ID that matches your Passkey/FIDO2 token that was also used when you installed the AD FS Adapter 13.0 for Entrust Identity Enterprise. See Install AD FS Adapter for Entrust Identity Enterprise.

Register Passkey/FIDO2 token with Entrust Identity Self-Service Module

Registering Passkey/FIDO2 token

1. Before you begin, locate your Passkey/FIDO2 token that is compliant with compliant with the FIDO2/WebAuthn specification.
2. Log in to the Entrust Identity Enterprise Self-Service Module portal. The **Self-Administration Actions** page appears.

3. Click **I'd like to register a passkey for authentication**.

4. Click **Yes** on the confirmation prompt. The **Register a Passkey for Authentication** page appears.

5. Enter a Passkey Name.

6. Click Register.

7. Follow the screen prompts to complete the Passkey/FIDO2 token registration.

Authenticate using Passkey/FIDO2 token

To authenticate using Passkey/FIDO2 token

1. Before you begin, locate your Passkey/FIDO2 token that is compliant with compliant with the FIDO2/WebAuthn specification.

2. Clear all browser cookies.

3. Access the AD FS resource and enter your username and password.

4. In the Challenge Authentication page, click Passkey.

5. A Remember me on this device pop-up appears.

server.mycompany.com   says

Would you like to enable "Remember me on this device" option?

OK   Cancel

6. To enable RBA, click **OK**. If you do not want to enable RBA, click **Cancel**.

7. Follow the screen prompts to complete Passkey/FIDO2 authentication.

Configure AD FS with Microsoft 365 for multifactor authentication

This section describes how to configure AD FS Adapter 13.0 with Microsoft 365 for multifactor authentication.

Prerequisites

Before you begin, complete the following prerequisites:

1. Add a domain to Microsoft 365 and make sure it is verified.

2. Configure AD FS for the same domain and install Entrust Identity AD FS Adapter.

3. Sync local Active Directory user accounts to Microsoft 365 using Microsoft Entra ID Connect.

4. [Sync Active Directory Users to IDaaS](#).

Connect AD FS to Microsoft 365

To connect AD FS to Microsoft 365, run the following commands in Windows Azure Directory Module for Windows PowerShell:

```
Enable-PSRemoting

$credentials = Get-Credential

Connect-MsolService -Credential $credentials

Set-MsolADFSContext –computer ADFSMachineName.SubDomain.Domain.com (FQDN)

Convert-MsolDomainToFederated -domain SubDomain.Domain.com -SupportMultipleDomain
```

If the commands run successfully, you should see the following message:

```
A "Microsoft 365 Identify Platform" Relying Party Trust is added to your AD FS
server.
```

Users who use the custom domain name as an email address suffix to log in to the Microsoft 365 portal are redirected to your AD FS server.

How to authenticate

1. Go to https://login.microsoftonline.com.
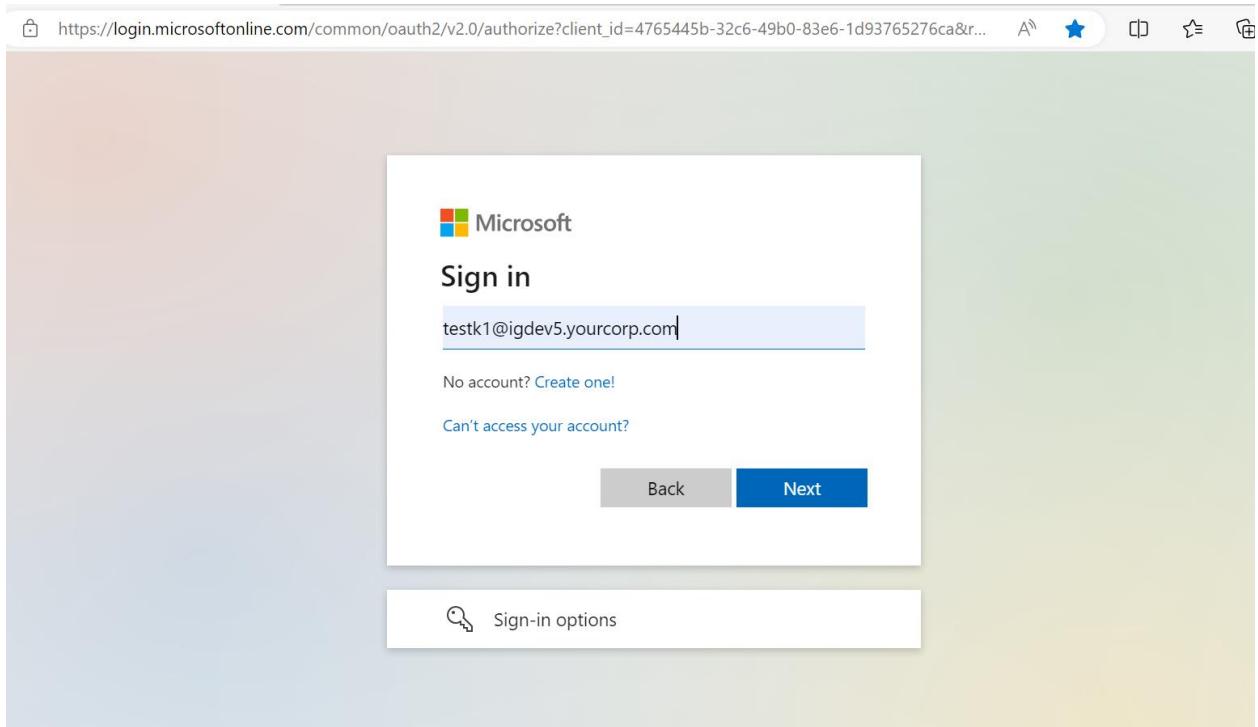
2. Enter the user account and click **Next**. You are prompted to enter the password.
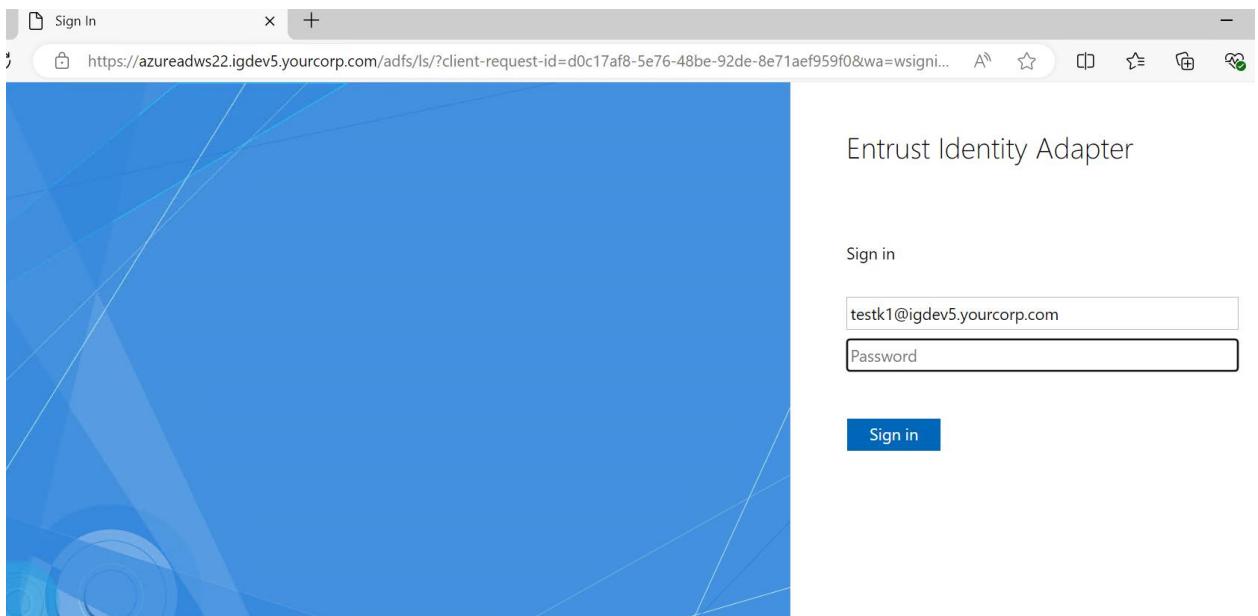
3. Enter the password and click **Sign in**. You are prompted to respond to a second-factor challenge.

Entrust Identity Adapter

For security reasons, we require additional information to verify your account

Entrust Challenge Authentication

To establish your identity, please respond to the following:

Enter a response to the grid challenge [B1] [E1] [E3] using a card with serial number: 10

These are the possible authentication types for this user:

Mobile Smart Credential
Mobile Soft Token
Token
One-Time Password
Question and Answer

4. Respond to the challenge successfully to be redirected to the protected resource.

Configure AD FS for Face Biometric authentication with IDaaS

Face Biometric authentication requires users to respond to the notification sent to their Identity App. A user can accept or reject the challenge, which results in either successful or failed authentication.

Note: This procedure assumes that you have already integrated AD FS with IDaaS. See Integrate AD FS Adapter in the *Technical Integrations Guides* for more information.

To configure AD FS for Face Biometric with IDaaS

1. Configure Face Biometric for multifactor authentication. See Manage Face Biometrics by Onfido section in the IDaaS *Administrator Help*.

2. Create a custom user login **Authentication Flow** to enable Face Biometric for second-factor authentication. See Create authentication flows in the *IDaaS Administrator Help*.

3. Create a resource rule that includes the Authentication Flow that enables Face Biometric for second-factor authentication. See Create a resource rule in the IDaaS *Administrator help*.

Note: ADFS supports Face biometric authentication only.

Authenticate using a Face Biometric token

To authenticate using face biometrics

1. Access the AD FS resource and enter your username and password.

2. In the second-factor page, the Face Biometric challenge appears..
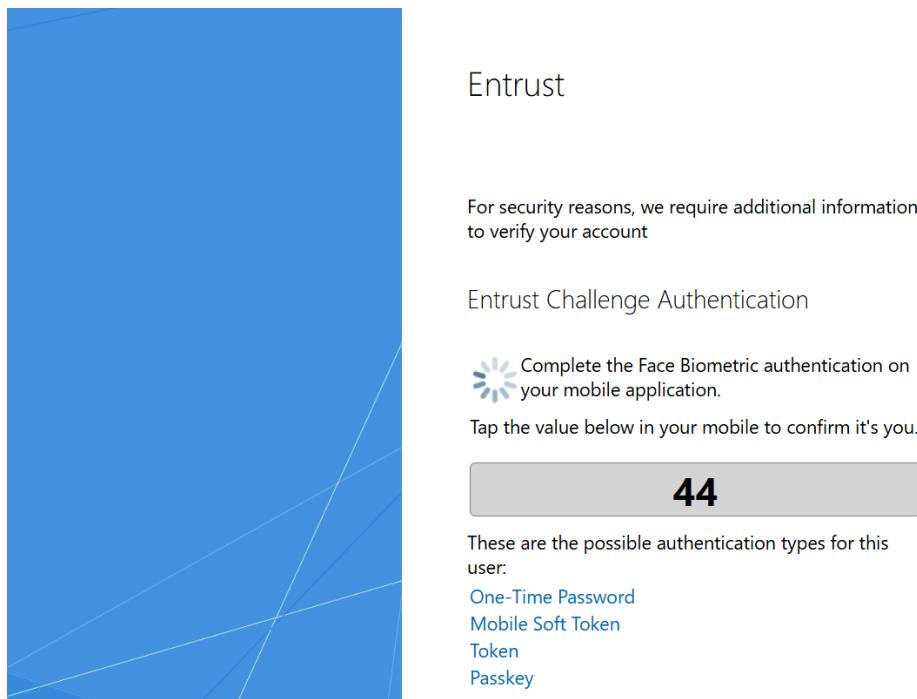
3. The user receives the notification on their mobile device in the Entrust Identity app.

4. The user clicks the value that appears on the resource second-factor authentication page.
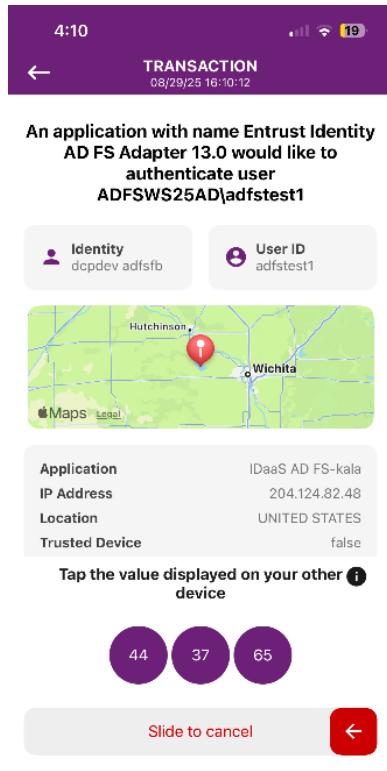
5. The **Record a video** screen appears.
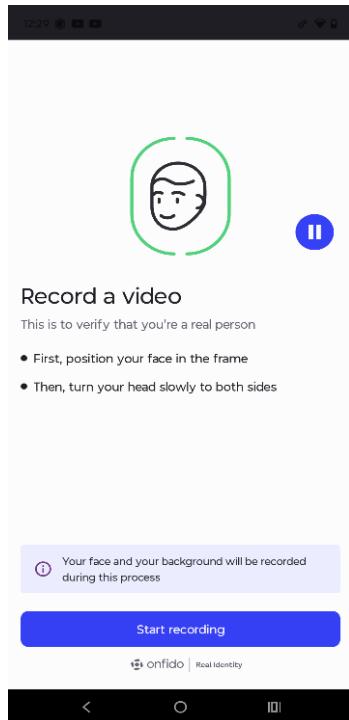
6. The user clicks **Start Recording** and proceeds with face recording.

7. The user is redirected to the resource page on successful authentication.

Include location information in the Entrust Identity app

To include location information in the transaction details of the Entrust Identity app, you need to configure this option in the AD FS application in IDaaS.

To include location information in the Entrust Identity app

1. Edit the AD FS application in IDaaS. (See Integrate AD FS Adapter in the IDaaS *Technical Integration Guides*.)

2. Set **Source of Client IP Address for Resource Rule Risk Factors and Audits** to **From the incoming HTTP connection**.

3. Save the changes.

Testing the integration

Before you test your integration, you must create a user in Entrust Identity Enterprise or Identity as a Service and assign an authenticator to the user. After doing so, you should be able to access the WAP published.

To test the integration

1. Go to the starting page for the sample WAP application, for example, `https://igadfsplugin.mydomain.com/claimapp`. WAP redirects to AD FS for first factor authentication.

    The First Factor authentication page appears.
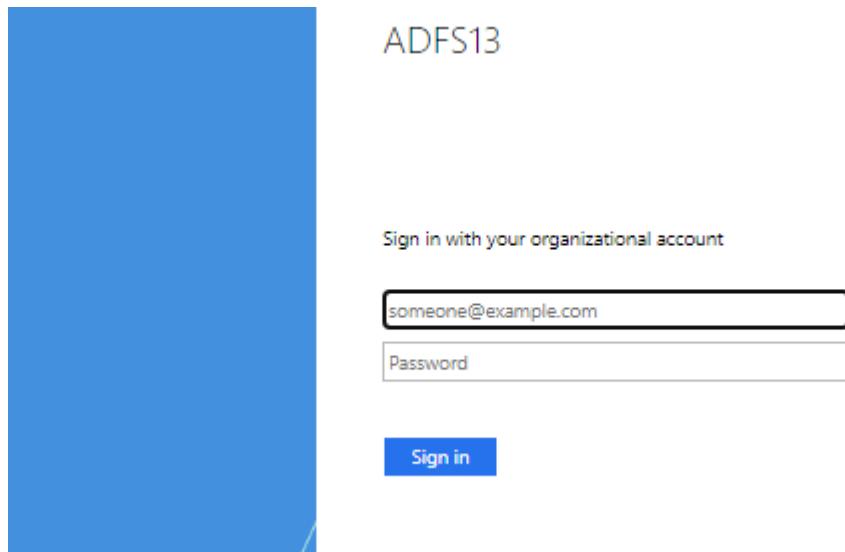
2. Enter your userID and password and click **Sign in**.

    The Entrust Identity AD FS Adapter second-factor authentication page appears.

ADFS13

For security reasons, we require additional information to verify your account
(tes...)

Entrust Challenge Authentication

To establish your identity, please respond to the following:

Enter a response to the grid challenge [C1] [C5] [I2] using a card with serial number: 3

These are the possible authentication types for this user:

Mobile Soft Token
Token
Mobile Smart Credential
One-Time Password
Question and Answer

Use temporary PIN

Submit

☐ Remember me on this device

ENTRUST

3. Enter your second factor authentication.

After successful authentication, a security token is returned with the claim, which WAP is expecting from AD FS and the Resource page appears.

The WAP sample application resource page.

Welcome : IGW2019\testvpn1
Values from IIdentity

| IsAuthenticated:True | Name:IGW2019\testvpn1 |

Claims from IClaimsIdentity

Claim Type	Claim Value	Value Type	Subject Name	Issuer Name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/implicitupn	testvpn1@igw2019.com	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2017/04/identity/claims/riskscore	notevaluated	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2017/04/identity/claims/accountthrottled	false	boolean	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/claims/authnmethodsproviders	FormsAuthentication	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/claims/authnmethodsproviders	EntrustDatacardADFSPlugin	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2014/01/identity/claims/anchorclaimtype	http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	testvpn1@igw2019.com	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid	S-1-5-21-765353213-911776581-3481696992-513	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid	S-1-5-21-765353213-911776581-3481696992-1111	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	IGW2019\testvpn1	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname	IGW2019\testvpn1	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2017/04/identity/claims/multifactorauthenticationinstant	2019-04-24T17:42:43.509Z	dateTime	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/claims/authnmethodsreferences	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.com/ws/2012/12/authmethod/identityguard	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.com/claims/multipleauthn	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-21-765353213-911776581-3481696992-513	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-1-0	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-32-545	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-2	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-11	string	IGW2019\testvpn1	http://nlb.igw2019.com/adfs/services/trust

Post-installation configuration

After installing the Entrust Identity AD FS Adapter, you complete the following post-installation tasks, as required. This section includes the following topics:

- [Configuring AD FS for Identity as a Service](#)
- [Configuring AD FS for Entrust Identity Enterprise](#)
- [Configuring the second factor authentication method](#)
- [Configuring alternate authenticators](#)
- [Configuring the user domain to Entrust Identity Enterprise group mapping](#)
- [Migrating users to Entrust Identity Enterprise](#)
- [Customizing end-user messages](#)
- [Configuring logging](#)

Configuring AD FS for Identity as a Service

You need to configure the Authentication API to allow authentication using Identity as a Service.

To configure for Identity as a Service authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Set the AuthenticationAPI element to `IntelliTrust`.

   This setting is used to make REST calls to Identity as a Service and to validate the second factor authenticators against Identity as a Service.

   a. To configure the `AuthenticationAPI`, locate the following:

      `<AuthenticationAPI></AuthenticationAPI>`

   b. Change the Authentication API as follows:

      `<AuthenticationAPI>IntelliTrust</AuthenticationAPI>`

4. Configure the `Application ID`.

   The `Application ID` is the unique identifier of the Identity as a Service authentication API application. This is ID is created in Identity as a Service when you add AD FS as an authentication API to Identity as a Service.

   a. To configure the ApplicationID, locate the following:

      `<ApplicationID></ApplicationID>`

   b. Add the `ApplicationID` created in Identity as a Service. For example:

      `<ApplicationID>1d123f45-d5c8-45f5-a614-e3f123c45be6</ApplicationID>`

5. Save and close `eigadfsplugin.xml`.

6. Restart Active Directory Federation Services.

Configuring AD FS for Entrust Identity Enterprise

You need to configure the Authentication API to allow authentication using Entrust Identity Enterprise.

To configure for Entrust Identity Enterprise authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Set the AuthenticationAPI element to `IdentityGuard`.

   This setting is used to make SOAP calls to Identity as a Service and to validate the second factor authenticators against Identity as a Service.

   a. To configure the `AuthenticationAPI`, locate the following:

      `<AuthenticationAPI></AuthenticationAPI>`

   b. Change the Authentication API as follows:

      `<AuthenticationAPI>IdentityGuard</AuthenticationAPI>`

4. Provide the Entrust Identity Enterprise server and config elements. See Configuring the second factor authentication method.

5. Save and close `eigadfsplugin.xml`.

6. Restart Active Directory Federation Services.

Configuring the second factor authentication method

After installation you can change the second factor authentication by editing the `eigadfsplugin.xml` file.

Note: For your changes to take effect, you must comment the authentication second factor method you no longer want to use and uncomment the new authentication method in the `eigadfsplugin.xml` file.

For example, if during installation you chose grid as the second factor authentication method but you want to replace it with another method, such as policy, be sure to comment the definition for grid and uncomment the definition for policy to ensure that your changes are applied.

This section contains the following topics:

- Configuring policy-based authentication
- Configuring grid authentication
- Configuring token authentication
- Configuring knowledge-based authentication
- Configuring policy authentication to override Q&A challenge size
- Configuring one-time password (OTP) authentication
- Configuring Mobile Smart Credential authentication (Identity Assured)
- Configuring Mobile Soft Token (TVS) authentication
- Configuring Passkey/FIDO2

Configuring policy-based authentication

You can use policy-based authentication as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file.

To configure policy-based authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

   ```
   <AuthenticationMethods>

           ...

   </AuthenticationMethods>
   ```

4. Define an `AuthMethod` element as shown in the example below.

   ```
   <AuthMethod id="Policy">
         <Authenticator>
         <Policy/></Authenticator>
   </AuthMethod>
   ```

5. Be sure to uncomment the `policy` definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

Configuring grid authentication

You can use grid authentication as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file. Additionally, you can configure grid to specify an enhanced RBA and a particular Entrust Identity Enterprise group.

To configure grid authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

   ```
   <AuthenticationMethods>

           ...

   </AuthenticationMethods>
   ```

4. Define an `AuthMethod` element as shown in the example below.

   ```
   <AuthMethod id="Grid">
         <Authenticator>
               <Grid/>
         </Authenticator>
         <RBA>
               <SecurityLevel>normal</SecurityLevel>
               <UseIP>false</UseIP>
               <RegisterMachine>
   ```

```
                <UseMachineNonce enabled="false" cookieName="machineNonce"
        cookieDomain="{cookiedomain}" cookieLifetime="365" />
                <UseSequenceNonce enabled="false"
        cookieName="sequenceNonce" cookieDomain="{cookiedomain}"
        cookieLifetime="365" />
                <UseAppData>false</UseAppData>
            </RegisterMachine>
        </RBA>
    </AuthMethod>
```

5. Be sure to uncomment the `grid` definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

To configure grid for enhanced RBA

8. Stop Active Directory Federation Services.

9. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

10. Locate the `AuthenticationMethods` element.

```
    <AuthenticationMethods>

            ...

    </AuthenticationMethods>
```

11. Define an `AuthMethod` element as shown in the example below.

```
    <AuthMethod id="GridRBA">
        <Authenticator>
                <Grid/>
        </Authenticator>
        <RBA>
                <SecurityLevel>enhanced</SecurityLevel>
                <UseIP>false</UseIP>
                <RegisterMachine>
                    <UseMachineNonce enabled="false" cookieName="machineNonce"
        cookieDomain="{cookiedomain}" cookieLifetime="365" />
                    <UseSequenceNonce enabled="false"
        cookieName="sequenceNonce" cookieDomain="{cookiedomain}"
        cookieLifetime="365" />
                    <UseAppData>true</UseAppData>
                </RegisterMachine>
            </RBA>
    </AuthMethod>
```

12. Be sure to uncomment the applicable definition strings.

13. Save and close `eigadfsplugin.xml`.

14. Restart Active Directory Federation Services.

Configuring token authentication

You can use token as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file.

To configure token authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

   ```
   <AuthenticationMethods>

        ...

   </AuthenticationMethods>
   ```

4. Define an `AuthMethod` element as shown in the example below.

   ```
   <AuthMethod id="Token">
        <Authenticator>
             <Token/>
        </Authenticator>
     <RBA>
          <SecurityLevel>normal</SecurityLevel>
             <UseIP>false</UseIP>
          <RegisterMachine>
             <UseMachineNonce enabled="false" cookieName="machineNonce"
   cookieDomain="{cookiedomain}" cookieLifetime="365" />
             <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
   cookieDomain="{cookiedomain}" cookieLifetime="365" />
             <UseAppData>false</UseAppData>
          </RegisterMachine>
     </RBA>
   </AuthMethod>
   ```

5. Be sure to uncomment the token definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

Configuring knowledge-based authentication

You can use knowledge-based as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file. Additionally, you can configure knowledge-based authentication to override the default question and answer challenge size.

To configure knowledge-based authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

   ```
   <AuthenticationMethods>

        ...

   </AuthenticationMethods>
   ```

4. Define an `AuthMethod` element as shown in the example below.

```
<AuthMethod id="KB">
 <Authenticator>
        <KB/>
 </Authenticator>
 <RBA>
        <SecurityLevel>normal</SecurityLevel>
        <UseIP>flase</UseIP>
        <RegisterMachine>
                <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
                <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
                <UseAppData>false</UseAppData>
        </RegisterMachine>
 </RBA>
</AuthMethod>
```

5. Be sure to uncomment the `KB` definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

To configure knowledge-based authentication and override the default question and answer challenge size

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

```
<AuthenticationMethods>

        ...

</AuthenticationMethods>
```

4. Define an `AuthMethod` element as shown in the example below.

```
<AuthMethod id="KBOverrideSize">
 <Authenticator>
        <KB>
                <OverrideKBChallengeSize size="4" />
                <MaskAnswers>false</MaskAnswers>
        </KB>
 </Authenticator>
 <RBA>
        <SecurityLevel>normal</SecurityLevel>
        <UseIP>false</UseIP>
                <RegisterMachine>
                <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
                <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
                <UseAppData>false</UseAppData>
        </RegisterMachine>
 </RBA>
</AuthMethod>
```

5. Be sure to uncomment the applicable definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

Configuring policy authentication to override Q&A challenge size

You can configure policy authentication to override the default question and answer challenge size if knowledge-based is chosen for the user.

To configure policy authentication and override the default question and answer challenge size

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

```
<AuthenticationMethods>

        ...

</AuthenticationMethods>
```

4. Define an `AuthMethod` element as shown in the example below.

```
<AuthMethod id="PolicyOverrideSize">
       <Authenticator>
             <Policy>
                 <OverrideKBChallengeSize size="4">
                 <MaskAnswers>false</MaskAnswers>
                 <AllowManualDelivery>false</AllowManualDelivery>
             </Policy>
      </Authenticator>
      <RBA>
           <SecurityLevel>normal</SecurityLevel>
           <UseIP>false</UseIP>
           <RegisterMachine>
               <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
               <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
           <UseAppData>false</UseAppData>
          </RegisterMachine>
    </RBA>
</AuthMethod>
```

5. Be sure to uncomment the applicable definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

Configuring one-time password (OTP) authentication

You can use one-time password as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file.

To configure OTP authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

```
<AuthenticationMethods>

      ...

</AuthenticationMethods>
```

4. Define an `AuthMethod` element as shown in the example below.

```
<AuthMethod id="OTP">
  <Authenticator>
        <OTP>
          <AllowManualDelivery>false</AllowManualDelivery>
        </OTP>
  </Authenticator>
  <RBA>
        <SecurityLevel>normal</SecurityLevel>
        <UseIP>false</UseIP>
        <RegisterMachine>
              <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
              <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
              <UseAppData>false</UseAppData>
        </RegisterMachine>
  </RBA>
</AuthMethod>
```

5. Be sure to uncomment the `OTP` definition strings.

6. To enable default OTP delivery for users under Identity Enterprise, add `AllowDefaultDelivery` configuration setting inside OTP Authenticator as shown below.

   <OTP>

     <AllowDefaultDelivery>true</AllowDefaultDelivery>

   </OTP>

   Note: If you are using a Policy Authenticator, add the AllowDefaultDelivery configuration setting inside the Policy Authenticator as shown below.

   <Policy>

     <AllowDefaultDelivery>true</AllowDefaultDelivery>

   </Policy>

7. Enable optional display and masking of information values in OTP challenges, as shown below:

`<IdentityGuardV11ExSupportRequired>true</IdentityGuardV11ExSupportRequired>`

   By default, this element is set to `false`.

Note: Identity as a Service is not supported if this setting is set to `true`.

When users initiate the sending of one-time passwords (OTP) to be used for authentication, they choose the email or phone number to which the OTPs should be sent. This feature shows the contact information values (with masking) in addition to generic labels such as *Work Email* and *Work Phone*. For details, see "Set policies for out-of-band OTPs" in the *Entrust Identity Enterprise Server Administration Guide*.

8. Save and close `eigadfsplugin.xml`.

9. Restart Active Directory Federation Services.

Configuring Mobile Smart Credential authentication (Identity Assured)

You can use Mobile SC as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file.

To configure Mobile SC authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

   ```
   <AuthenticationMethods>

           ...

   </AuthenticationMethods>
   ```

4. Define an `AuthMethod` element as shown in the example below.

   ```
   <AuthMethod id="MobileSC">
     <Authenticator>
           <MobileSC pollingInterval="2"/>
     </Authenticator>
     <RBA>
           <SecurityLevel>normal</SecurityLevel>
           <UseIP>false</UseIP>
           <RegisterMachine>
                   <UseMachineNonce enabled="false" cookieName="machineNonce"
   cookieDomain="{cookiedomain}" cookieLifetime="365" />
                   <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
   cookieDomain="{cookiedomain}" cookieLifetime="365" />
                   <UseAppData>false</UseAppData>
           </RegisterMachine>
     </RBA>
   </AuthMethod>
   ```

5. Be sure to uncomment the `MobileSC` definition strings.

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

Configuring Mobile Soft Token (TVS) authentication

You can use Mobile ST as your second-factor authentication type by editing the Entrust Identity AD FS Adapter configuration file.

To configure Mobile ST authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the `AuthenticationMethods` element.

   ```
   <AuthenticationMethods>
   ```

```
            . . .
        </AuthenticationMethods>
```

4. To enable automatic fall back from Mobile Soft Token (TVS) Authentication to Token Authenticaiton, set define an `AuthMethod` element as shown in the example below.

```
<AuthMethod id="MobileST">
    <Authenticator>
        <MobileST pollingInterval="2" mode="Online" fallbackToClassic="true"/>
    </Authenticator>
    <RBA>
        <SecurityLevel>normal</SecurityLevel>
<UseIP>false</UseIP>
        <RegisterMachine>
            <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
            <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
            <UseAppData>false</UseAppData>
        </RegisterMachine>
    </RBA>
</AuthMethod>
```

5. To disable automatic fallback from Mobile Soft Token (TVS) authentication to token authentication, define an `AuthMethod` as shown in the following example:

```
<AuthMethod id="MobileST">
    <Authenticator>
        <MobileST pollingInterval="2" mode="Online" fallbackToClassic="false"/>
    </Authenticator>
    <RBA>
        <SecurityLevel>normal</SecurityLevel>
<UseIP>false</UseIP>
        <RegisterMachine>
            <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
            <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />
            <UseAppData>false</UseAppData>
        </RegisterMachine>
    </RBA>
</AuthMethod>
```

6. Be sure to uncomment the `MobileST` definition strings.

7. Save and close `eigadfsplugin.xml`.

8. Restart Active Directory Federation Services.

Configuring Passkey/FIDO2

To configure passkey/FIDO2 authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. For the following settings, refer to the settings you used when you installed Entrust Identity AD FS Adapter for Entrust Identity Enterprise. See Step 16 on page 19.

c. Locate the `RelyingPartyID` and enter the Relying Party ID you used when you installed the Entrust Identity AD FS Adapter 13.0. For example:

```
<RelyingPartyID>mycompany.com</RelyingPartyID>
```

d. Locate the `PasskeyOrigin` and enter the Passkey value. For example:

```
<PasskeyOrigin>https://<clustername>.<domain_name>.mycompany.com</PasskeyOrigin>
```

e. Locate `AllowOriginSubDomain` and set it to either `true` or `false`. For example:

```
<AllowOriginSubDomain>true</AllowOriginSubDomain>
```

4. Locate `AllowOriginPort` and set it to `True` or `False` based on the TLS configuration.

```
<AllowOriginPort>false</AllowOriginPort>
```

5. Locate the `AuthenticationMethods` element.

```
<AuthenticationMethods>

                ...

</AuthenticationMethods>
```

6. Define an `AuthMethod` element as shown in the example below.

```
<AuthMethod id="Passkey">

        <Authenticator>

             <Passkey/>

        </Authenticator>

   <RBA>

        <SecurityLevel>normal</SecurityLevel>

            <UseIP>false</UseIP>

        <RegisterMachine>

            <UseMachineNonce enabled="false" cookieName="machineNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />

            <UseSequenceNonce enabled="false" cookieName="sequenceNonce"
cookieDomain="{cookiedomain}" cookieLifetime="365" />

            <UseAppData>false</UseAppData>

        </RegisterMachine>

   </RBA>

</AuthMethod>
```

7. Be sure to uncomment the passkey definition strings.

8. Save and close `eigadfsplugin.xml.`

9. Restart Active Directory Federation Services.

Configuring alternate authenticators

To have a link for an alternate authenticator appear on the login screen for a given user, that authenticator must:

- be configured for use in the policy for the Entrust Identity Enterprise group to which the user belongs
- be an authenticator that the user possesses (for example a grid card, knowledge of the answers to questions, or a mobile smart credential)
- be configured as an alternate authentication method for a given `<AuthenticationMethod>` in the `eigadfsplugin.xml` file

You can configure the Entrust Identity AD FS Adapter to display alternative second-factor authenticators on the second-factor authentication page (see Figure 2: Alternative authenticators)**.** Users can select an alternative if they do not have their primary authenticator.

The following authenticators are supported as alternatives:

- grid
- token
- knowledge-based Q&A
- one-time password (OTP)
- MobileSC
- MobileST
- Passkey

For example, Q&A will be visible as an alternative even if the user has not created Q&A answers yet, if you allowed Q&A in your policy and it is configured in the configuration file.

Figure 2: Alternative Authenticators

To enable alternative authenticators

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Locate the authenticator that will be an alternative authenticator. For example, locate this XML block:

    ```
    <AuthMethod id="gridAuth">
      <Authenticator>
         <Grid />
      </Authenticator>
    </AuthMethod>
    ```

4. Add the following text, in bold:

    ```
    <AuthMethod id="gridAuth">
      <Authenticator>
        <Grid Alternate="true"/>
    ```

```
<Token Alternate="true"/>
<OTP Alternate="true" />
  <AllowManualDelivery>false</AllowManualDelivery>
</OTP>
<KB Alternate="false">
 <OverrideKBChallengeSize size="4" />
 <MaskAnswers>false</MaskAnswers>
</KB>
<MobileSC Alternate="true"/>
</Authenticator>
</AuthMethod>
```

where `Alternate=true` indicates that the authenticator must be listed as a link below the primary authenticator, if it is not already displayed as the primary authenticator.

5. Save and close `eigadfsplugin`.xml.

6. Restart Active Directory Federation Services.

Configuring IP Geo risk-based authentication

To configure IP Geo risk-based authentication

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

3. Find the `AuthMethod` element that you want to define for the IP Geo risk-based authentication settings.

   For example:

   `<AuthMethod id="Grid">`

   `<Authenticator>`

   `<Grid/>`

   `</Authenticator>`

   `</AuthMethod>`

3. Add an RBA element immediately after the closing Authenticator tag in the `AuthMethod` definition to which you want to add risk-based authentication.

```
<AuthMethod id="Grid">
    <Authenticator>
        <Grid/>
    </Authenticator>
        <RBA>
        ...
        </RBA>
</AuthMethod>
```

4. Add child elements as needed to the RBA element.

5. Add the `UseIP` element (optional) and set it to `true` if you want to pass the client IP address to Entrust Identity Enterprise for IP Geolocation analysis.

```
<RBA>

        <SecurityLevel>Normal</SecurityLevel>

        <UseIP>true</UseIP>

        ...

</RBA>
```

6. Save and close `eigadfsplugin.xml`.

7. Restart Active Directory Federation Services.

Configuring the user domain to Entrust Identity Enterprise group mapping

Entrust Identity AD FS Adapter supports mapping a domain from AD FS primary authentication to a corresponding group in Entrust Identity Enterprise Server. By default, the Entrust Identity Enterprise group is not used.

Group configuration is optional. If there is no group configuration, there is no Entrust Identity Enterprise group passed to the Entrust Identity Enterprise Server and all groups are searched for the user.

To configure user domain to Entrust Identity Enterprise group mapping

8. Stop Active Directory Federation Services.

9. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

10. Add the following block of text to the text file:

```
<Group useDomain="true" useThisGroup="IGGroup">

  <DomainToGroupMapping domainName="ADFS1" groupName="IGGroup1" />

  <DomainToGroupMapping domainName="ADFS2" groupName="IGGroup2" /> </Group>
```

where

- If `useThisGroup` is present, the value of `useThisGroup` Entrust Identity Enterprise group is taken as first priority and all other strings are ignored.

- If `useDomain` is present and if it is `false`, no Entrust Identity Enterprise Group is used.

- If `useDomain` is present and if it is `true`, the domain from AD FS first factor authentication is searched in the list of available `DomainToGroupMapping` nodes.

- If any `domainName` in `DomainToGroupMapping` matches the incoming AD FS first factor domain, the corresponding groupName will be used as IG Group.

- If no `domainName` in `DomainToGroupMapping` is matched, then same incoming AD FS first factor domain is used as IG Group.

   Note: `domainName`, `groupName` referred in `DomainToGroupMapping` are case insensitive.

11. Save and close `eigadfsplugin.xml`.

12. Restart Active Directory Federation Services.

Migrating users to Entrust Identity Enterprise or Identity as a Service

User migration is the process of making all your end users of Entrust Identity Enterprise or Identity as a Service users who access your protected resources through the AD FS Adapter. The AD FS Adapter has user migration features that you can configure to allow your users to continue to access your protected resources while you deploy your solution.

You can either force or phase in migration.

Forcing migration

In this scenario, after you install the AD FS Adapter, you force all users to enroll with Entrust Identity Enterprise and to activate a second-factor authentication method. Until users complete the enrollment, they cannot access protected resources.

Forced migration works well when you have a small number of end users. It is recommended that you implement a cutoff date before which all users must complete the enrollment.

If you have a large number of end users, they could all attempt the migration at once, causing heavy demand on your servers. To avoid this problem, you may want to a phased approach to migration (see "Phasing in migration").

To set fallback to Entrust Identity Enterprise

If your users exist in Entrust Identity Enterprise but not Identity as a Service and you have set the `AuthenticationAPI` to `IntelliTrust` but you want to set fallback authentication to Entrust Identity Enterprise, you need to set the `<AllowFallbackToIG>` to true.

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

   a. Locate `<AllowFallbackToIG></AllowFallbackToIG>`

   - If `AllowFallbackToIG` is `true` and if the user exists in Identity as a Service, continue MFA using the Identity as a Service API, if not fall back to Entrust Identity Enterprise. The Entrust Identity Enterprise user is not enrolled in the Identity as a Service Admin Portal but the user wants to access the protected resources through AD the FS 5.0 Adapter.

   - If `AllowFallbackToIG` is `false` and if the user exists in Identity as a Service, continue MFA using Identity as a Service API, if not show an error message. The Entrust Identity Enterprise user is not enrolled in the Identity as a Service Admin Portal and you want to restrict access to the protected resources through AD FS Adapter.

3. Save and close `eigadfsplugin.xml`.

4. Restart Active Directory Federation Services.

To implement forced migration

1. Create Entrust Identity Enterprise or Identity as a Service user IDs for all your end users.

2. Stop Active Directory Federation Services.

3. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file.

4. Modify the `<UserMigration>` element in the file as shown below:

   ```
   <SkipAuthNoExist enabled="false"
   <SkipAuthNoActive enabled="false"
   ```

5. Save and close `eigadfsplugin.xml.`

6. Restart Active Directory Federation Services.

7. Instruct your end users that they cannot access protected resources until they enroll with Entrust Identity Enterprise or Identity as a Service and activate a second-factor authentication method.

Phasing in migration

In this scenario, after you install the Entrust Identity AD FS Adapter, you force all users to enroll with Entrust Identity Enterprise or Identity as a Service and to activate a second-factor authentication method. Until they complete the enrollment, they cannot access protected resources.

To implement phased migration

1. Create Entrust Identity Enterprise user IDs for your first batch of users.

2. Have those users enroll in Entrust Identity Enterprise or Identity as a Service and assign second-factor authentication methods to them.

    -   For Entrust Identity Enterprise, you can enroll your users, or you can have them self-register using client software such as Entrust Identity Enterprise Self-Service Module or Entrust Desktop for Microsoft Windows.

    -   For Identity as a Service, you can create users or migrate users in bulk from Entrust Identity Enterprise or Active Directory.

    Note: Users who are already enrolled are not affected by the modifications described in the following steps.

3. Decide how you want the AD FS Adapter to handle the users who are not yet migrated.

4. Stop Active Directory Federation Services.

5. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the `eigadfsplugin.xml` file and modify the `<UserMigration>` section using the scenarios described below:

    -   If you want to block unmigrated users completely from the protected resource, set user migration as follows:

        ```
        <SkipAuthNoExist enabled="false"/>
        <SkipAuthNoActive enabled="false"/>
        ```

    -   If you want to allow unmigrated users unrestricted access to the protected resource, set user migration as follows:

        ```
        <SkipAuthNoExist enabled="true"/>
        <SkipAuthNoActive enabled="true" />
        ```

    -   If you want to redirect unrestricted users to another Web page, set user migration as follows:

        ```
        <SkipAuthNoExist enabled="true"
        url="https://adminigsss.mycorp.com:8445/IdentityGuardSelfService"/>
        <SkipAuthNoActive enabled="true"
        url="https://adminigsss.mycorp.com:8445/IdentityGuardSelfService"/>
        ```

        Note: Put in your own URL for the Web page, instead of the example shown above.

        There are other possible scenarios depending on how you want the AD FS Adapter to handle your unmigrated users. See "Modifying user migration" settings for the effect of each setting.

6. After you have migrated your first group of users, you can repeat steps 3-5 to migrate the next group.

7. Repeat until you have migrated all your users. After all your users are registered, you can disable the user migration feature, if desired, by changing the enabled attribute to false for both `<SkipAuthNoExist>` and `<SkipAuthNoActive>`.

8. Save and close `eigadfsplugin.xml`.

9. Restart Active Directory Federation Services.

Modifying user migration settings

When you deploy the AD FS Adapter, you may have end users in different states with regard to Entrust Identity Enterprise, as follows:

- Users may not have a user ID created in Entrust Identity Enterprise or Identity as a Service.

- Users may have a user ID created in Entrust Identity Enterprise, but do not yet have an Entrust Identity Enterprise or Identity as a Service password or second-factor authentication method assigned and activated.

- Users may have a user ID created in Entrust Identity Enterprise or Identity as a Service, and they have an Entrust Identity Enterprise or Identity as a Service password or second-factor authentication method assigned and activated.

The user migration settings in the authentication application configuration file allow you to choose how you handle the three types of users when they attempt to access a protected URL. User migration is configured globally for the entire solution. The user migration settings apply to all authentication methods in the solution.

You control the behavior of these features by modifying settings in the `<UserMigration>` element of `eigadfsplugin.xml`. The `<UserMigration>` element has two child elements:

- Modifying the `SkipAuthNoExist` element

- Modifying the `SkipAuthNoActive` element

Modifying the SkipAuthNoExist element

This element applies to users who have not yet been added to Entrust Identity Enterprise or Identity as a Service.

Users who have already been added in Entrust Identity Enterprise or Identity as a Service are not affected by the settings of this element.

`SkipAuthNoExist` has an attribute called enabled, which has two possible values: `true` or `false`. The default is `false`. It has the optional attribute `url`. You can use the element in several different ways.

If you set…	This is the effect…
`<SkipAuthNoExist enabled="false"/>`	Non-Entrust Identity Enterprise or Identity as a Service users are blocked from the protected resource. This is the default setting.
`<SkipAuthNoExist enabled="true"/>`	Non-Entrust Identity Enterprise or Identity as a Service users are allowed access to the protected resource without a second-factor challenge.

If you set…	This is the effect…
`<SkipAuthNoExist enabled="true" url="IdentityGuardEnrollment.aspx"/>`	Non-Entrust Identity Enterprise or Identity as a Service users are not allowed to access the protected resource, and they are redirected to the given URL. This URL could be a page informing the user to contact support, or a self-service interface for registering. The example shows the default page. It informs the user that they have not yet been enrolled in Entrust Identity Enterprise or Identity as a Service.

Modifying the SkipAuthNoActive element

This element applies to users who have been added to Entrust Identity Enterprise, but do not yet have any assigned and activated second-factor authentication methods, such as grid, token, Q&A, or OTP.

Users who already have activated second-factor methods are not affected by the settings of this element.

`SkipAuthNoActive` has an attribute called `enabled`, which has two possible values, `true` or `false`. The default is `false`. It has the optional attribute `url`. You can use the element in several different ways.

If you set…	This is the effect…
`<SkipAuthNoActive enabled="false"/>`	Entrust Identity Enterprise or Identity as a Service users who do not yet have assigned and activated second-factor authentication methods are blocked from the protected resource. This is the default setting.
`<SkipAuthNoActive enabled="true"/>`	Entrust Identity Enterprise or Identity as a Service users who do not yet have assigned and activated second-factor authentication methods are allowed access to the protected resource without a second-factor challenge.
`<SkipAuthNoActive enabled="true" url="IdentityGuardActivation.aspx"/>`	Entrust Identity Enterprise or Identity as a Service users who do not yet have assigned and activated second-factor authentication methods are not allowed to access the protected resource, and they are redirected to the given URL. This URL could be a page informing the user to contact support, or a self-service interface for registering. The example shows the default page informing the user that they do not yet have an active second-factor authentication method.

Customizing end-user messages

You can customize end user strings, errors, and other messages returned by the Entrust Identity Enterprise AD FS Adapter to meet your regional language requirements.

When a user makes a request to the AD FS server, the Entrust Identity AD FS Adapter fetches the user's browser language code and searches for the language-specific `Strings.resx` file.

Example of language-specific files:

- `Strings.resx` for English - shipped with the msi

- `Strings.de-DE.resx` for German (Germany) - shipped with the msi

- `Strings.fr.resx` for French (Standard)

- `Strings.da-DK.resx` for Danish (Denmark)

If the file is present in the installed location, the end-user messages are fetched from that file, If the file is not present, the end-user messages are fetched from the cached copy of the `Strings.resx` file.

Note: When the Entrust Identity AD FS Adapter is installed and the service is started or restarted, the `Strings.resx` file is cached in the Windows Server cache. This cache is not updated every time AD FS is restarted, After making changes to the `Strings.resx` file, restart the Entrust Identity AD FS Adapter to have the updated messages shown to users.

The Entrust Identity AD FS Adapter MSI is shipped with English and German versions of the `Strings.resx` files. Customization of end-user messages works as expected when users access AD FS from browsers with languages set to English or German.

To customize messages in English or German, complete the procedure To customize end-user messages in English or German.

To customize langages for users who will access the AD FS server from a browser set to a language other than English or German, complete the procedure To customize end-user messages in non-default languages.

To customize end-user messages in English or German

1. Stop Active Directory Federation Services.

2. Go to either `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` or `<adfs_adapter_install>\IntelliTrust ADFS Adapter\config` and open the `String.resx` file.

   This file contains all the Entrust Identity AD FS Adapter user messages.

3. Edit the messages as required.

4. Save and close `Strings.resx`.

5. Restart Active Directory Federation Services.

To customize end-user messages in non-default languages

1. Stop Active Directory Federation Services.

2. Open the `config\eigadfsplugin.xml` file, and search for the string "`<level value`".

3. Change the value of the string to `DEBUG`. It should look like this: `<level value="DEBUG" />`

4. Save and close `eigadfsplugin.xml` file.

5. Restart Active Directory Federation Services.

6. Make a request to AD FS server from a client browser and complete the request.

7. Go to Entrust Identity AD FS Adapter installation location and open the `log\EntrustADFS.log` file.

8. Search for the last entry of the string "`intializeGlobalResourceFile`" at the end of the file. You should see a debug log entry similar to the following line.

```
[DEBUG]
[EntrustDatacardAuthProvider.EIGAuthProviderAdapter.intializeGlobalResourceFile]
[session=none available] - Resource file is: C:\Program
Files\Entrust\IntelliTrust ADFS Adapter\Strings.da.resx
```

9. From the log, fetch the file name (in this example, it is `Strings.da.resx`) and create a new resx file with this file name by using the contents of `Strings.resx` file.

10. Edit the messages as required.

11. Save and close `Strings.resx`.

12. Restart Active Directory Federation Services.

Configuring logging

You can configure logging for the Entrust Identity AD FS Adapter independently. The Entrust Identity AD FS Adapter uses Apache logging packages to implement logging. The Entrust Identity AD FS Adapter uses Apache log4net 1.2.10. For more detailed information read the Apache documentation at:

http://logging.apache.org/log4net/release/sdk/log4net.Appender.RollingFileAppenderMembers.html

Location of log files

The log files are located at `C:\Program Files\Entrust\Identity Enterprise ADFS Adapter\log`.

Changing the logging level

You can configure the default logging level attribute for the Entrust Identity AD FS Adapter

The default logging level for the Entrust Identity AD FS Adapter is `INFO`. The possible values are:

- OFF
- FATAL
- ERROR
- WARN
- INFO
- DEBUG
- ALL

These levels show increasing amounts of information.

To change Entrust Identity AD FS Adapter logging level

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the eigadfsplugin.xml file.

3. Find the Logging element, and the level child element.

4. Change the value attribute to the level you want. The default is INFO. For example,

   `<level value="DEBUG" />`

5. Save and close `eigadfsplugin.xml`.

6. Restart Active Directory Federation Services.

The DEBUG and ALL log levels generate a lot of logs. When you have finished troubleshooting, set the logging level back to INFO to avoid slowing down your system.

Configuring the log file settings

You can configure the settings affecting the log files, such as the name of the log files, how many backups to keep, and so on.

To configure the log file settings for the Entrust Identity AD FS Adapter

1. Stop Active Directory Federation Services.

2. Go to `<adfs_adapter_install>\Identity Enterprise ADFS Adapter\config` and open the eigadfsplugin.xml file.

3. Locate the section that begins with:

   ```
   <!-- Logging settings for authentication provider -->
   ```

4. Modify the settings described below, depending on how you want to configure the log files.

   - `file`

     This setting specifies the name and location of the log file. For example:

     ```
     <file value="C:\Program Files\Entrust\Identity Enterprise ADFS
     Adapter\log\IdentityGuardADFS.log"/>
     ```

   - `appendToFile`

     This setting contains a Boolean value. If true, then new logging information is appended at the bottom of the log file. If false, then new logging information is written to a new log file, after renaming the previous log file by adding the suffix `.#` where `#` is an integer. For example, a log file named authapp.log is renamed to authapp.log.1 and a new authapp.log is created. For example:

     ```
     <appendToFile value="true" />
     ```

   - `maximumFileSize`

     This setting specifies the maximum size the log file can reach, before a new log file is created. When the log file reaches this size, it is renamed and a new log file is created. For example:

     `<maximumFileSize value="1000KB" />`

   - `maxSizeRollBackups`

     This setting specifies the number of backups of the log file to keep. Every time a new log file is created, all previous log files are renamed by adding the suffix `.#` where `#` is an integer. The value in this setting determines how many renamed files are kept before deleting. If 10 is specified, then 10 renamed files are kept as well as the active log file. Every time a new log file is created the oldest renamed file (with a .10 suffix) is deleted. For example:

     `<maxSizeRollBackups value="10" />`

   - `RollingFileAppender`

     Is the name of the appender that rolls log files based on size or date or both.

   - `rollingStyle`

     This sets the rolling style (meaning it will roll the log file based on size).

   - `staticLogFileName value="true"`

     Value attribute that indicates whether to always log to the same file.

   - `layout type="log4net.Layout.PatternLayout"`

     Type attribute that indicates the layout of log statements written in the log file.

   - `conversionPattern value="[%d] [%t] [%-5level] %m%n"`

     Value attribute that indicates the pattern/format of log statements written in the log file.

5. Save and close `eigadfsplugin.xml`.

6. Restart Active Directory Federation Services.

Upgrading Entrust Identity AD FS Adapter

Before upgrading the Entrust Identity AD FS Adapter, you must first deselect the Entrust Identity Enterprise Authentication Plugin from AD FS.

1. Go to the AD FS console and select Authentication Policies > Edit Global Multi-Factor Authentication. The Edit Authentication Methods page appears.
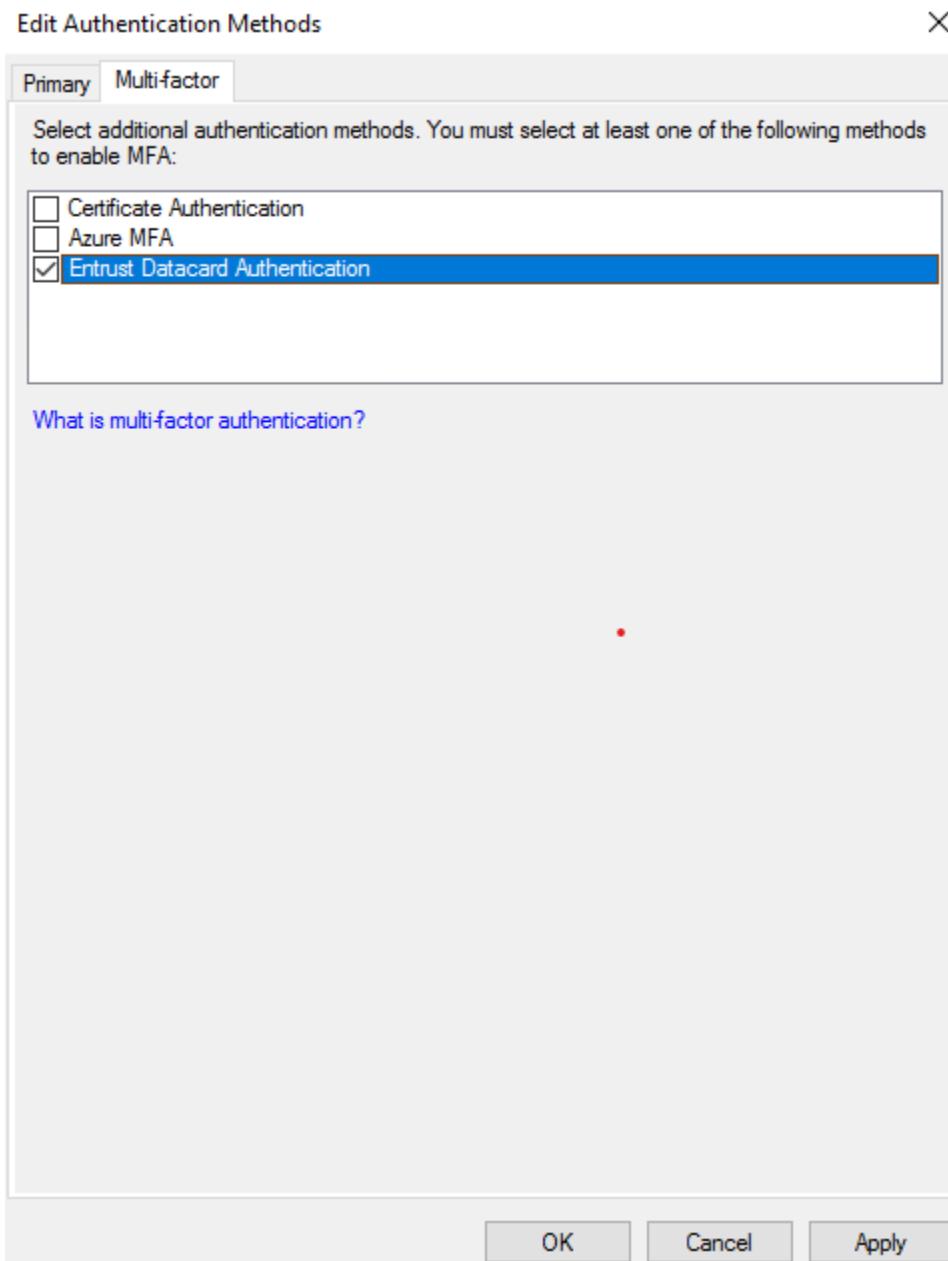
2. Follow the instructions in the section, Installing the Entrust Identity AD FS Adapter to complete the installation of the newer version.

3. Click **OK** on the Warning prompt.

Warning ✕

The backup of previous version files are stored at installation location i.e.,
C:\Program Files\Entrust\IDaaS ADFS Adapter\backup_10-8-2024\

OK

Note: Customizations will be present in the backup folder, but you must manually migrate the customizations to the newer version.

4. Click **Finish** to exit the Setup Wizard.

5. Restart the AD FS service.

Uninstalling the Entrust Identity AD FS Adapter

Before uninstalling the Entrust Identity AD FS Adapter, you must first deselect the Entrust Identity Enterprise Authentication Plugin from AD FS.

This section contains the following procedures:

To uninstall the Entrust Identity AD FS Adapter on Windows server 2022

1. Go to the AD FS console and select **Authentication Policies > Edit Global Multi-factor Authentication**.

   The Edit Authentication Methods page appears.
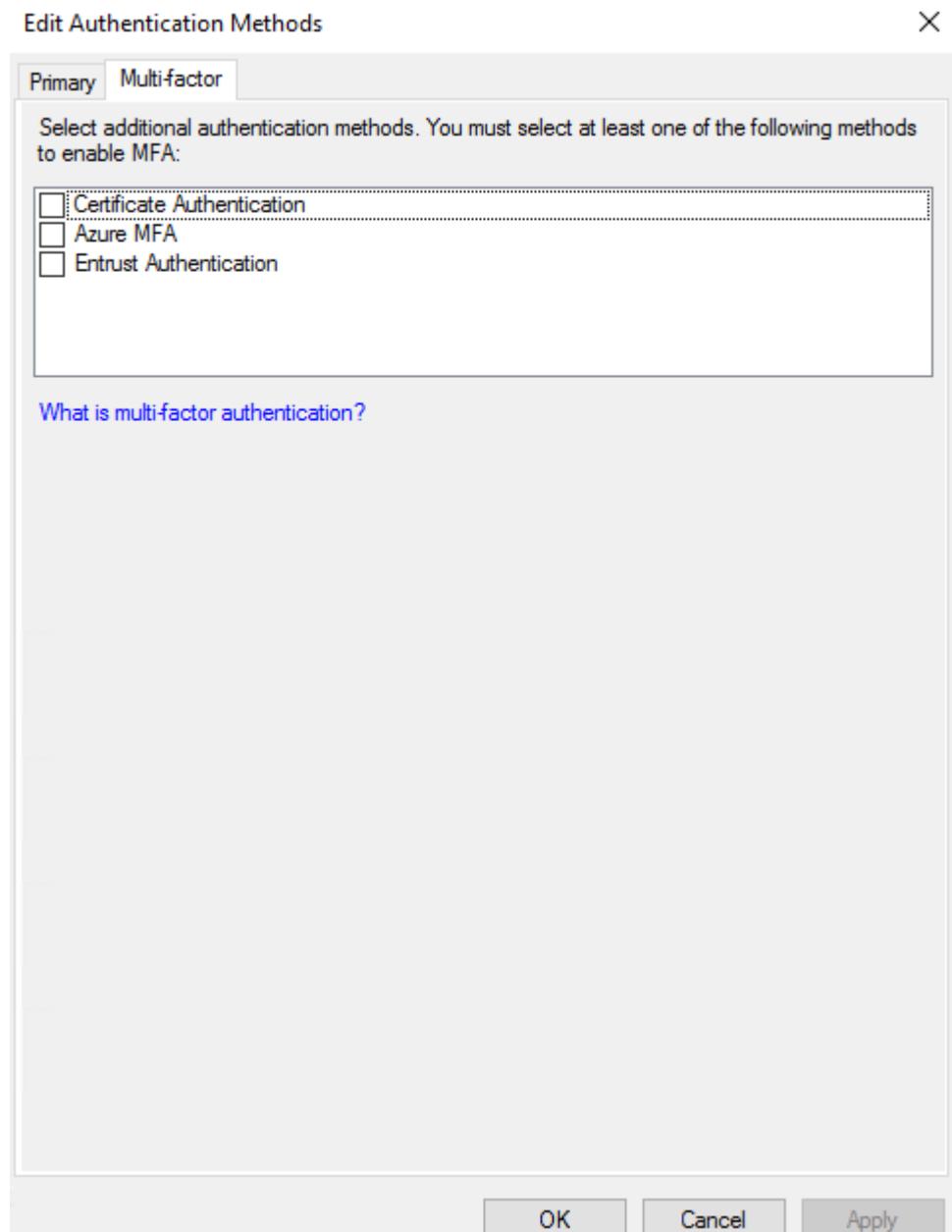
2. Uncheck **Entrust Authentication** and then click **OK**.

3. Go to **Control Panel > Programs > Uninstall a program** and double-click **Entrust Identity AD FS Adapter**. The AD FS Setup wizard opens.

A warning message appears reminding you to uncheck the **Entrust Authentication Plugin**.
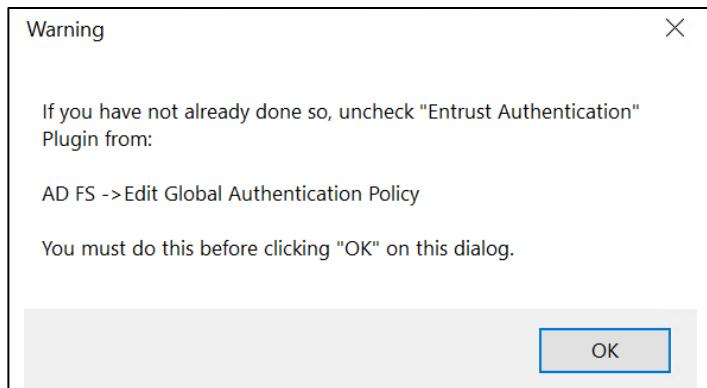

4. Click **OK** to complete the uninstall process.

   –or–

5. Double-click the `Entrust Identity AD FS Adapter 13.0` installer file. The Entrust Identity AD FS Adapter Setup Wizard appears.
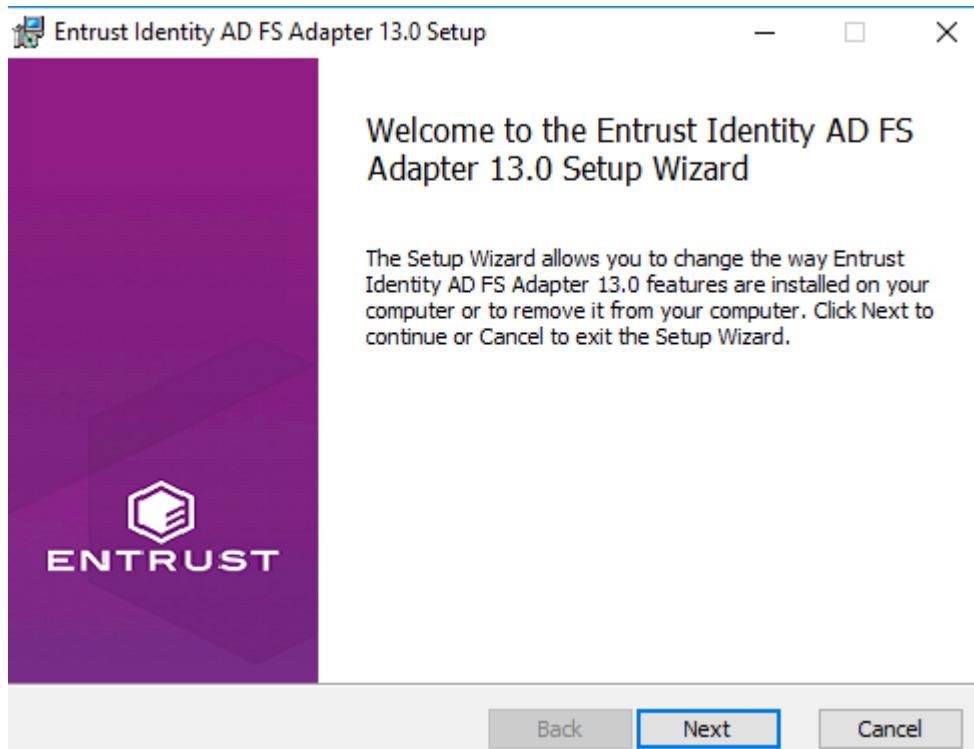

6. Click Next. The Change, Repair, or Remove Installation page appears.
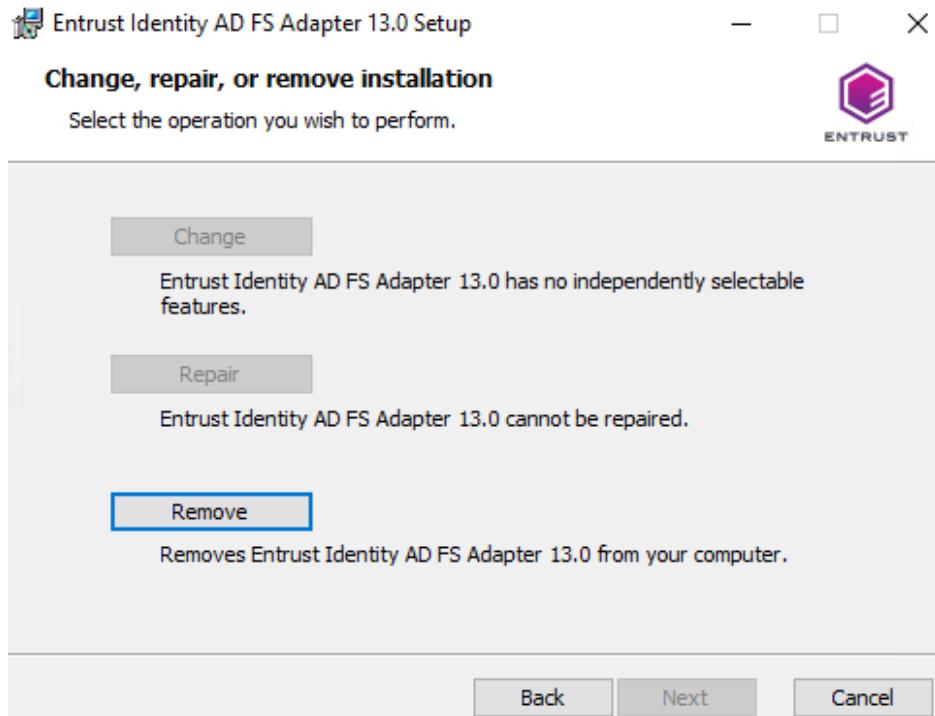
7. Click **Remove** and then click **Next**.

   A warning message appears reminding you to uncheck the Entrust Authentication Plugin
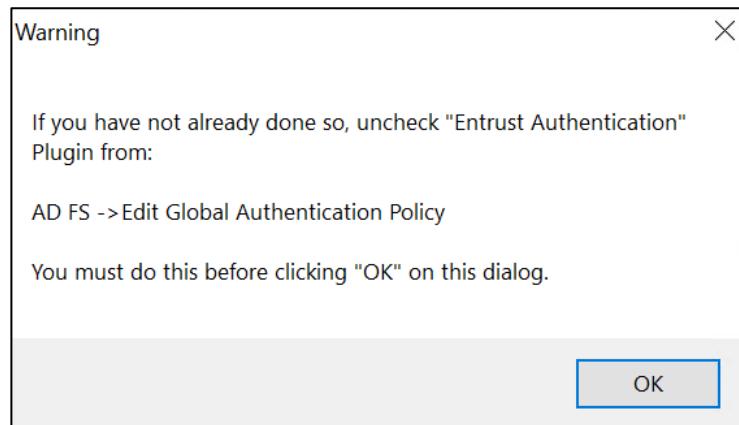
8. Click **OK** to complete the uninstall process.

   The Completed Entrust Identity AD FS Adapter Setup Wizard page appears.

9. Click **Finish** to exit the Setup Wizard. You must now restart your AD FS service.

Appendix A: Configuring AD FS

Configuring AD FS

The next step is to configure Active Directory Federation Services.

To configure AD FS 4.0 and 5.0

1. Start the AD FS configuration wizard from the server manager. The **AD FS Configuration Wizard** appears.

2. To start the AD FS Federation Server Configuration Wizard, do the following:

   a. After the Federation Service role service installation is complete, open the AD FS Management snap-in and click the **AD FS Federation Server Configuration Wizard** link on the **Overview** page or in the **Actions** pane.
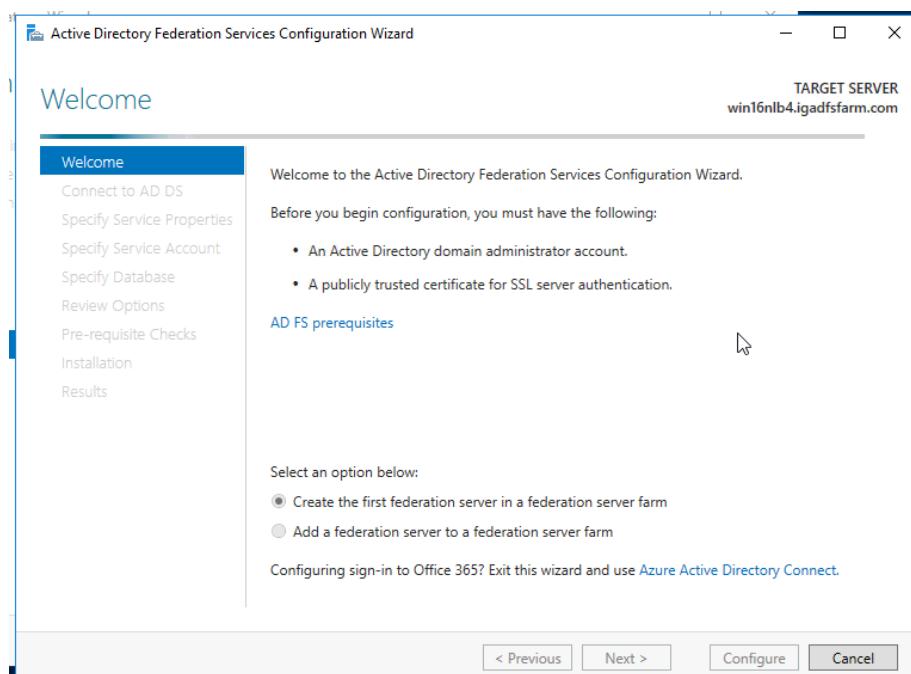
3. Click **Create the first federation server in a federation server farm** and then click **Next**. The Connect to Active Directory Domain Services page appears.
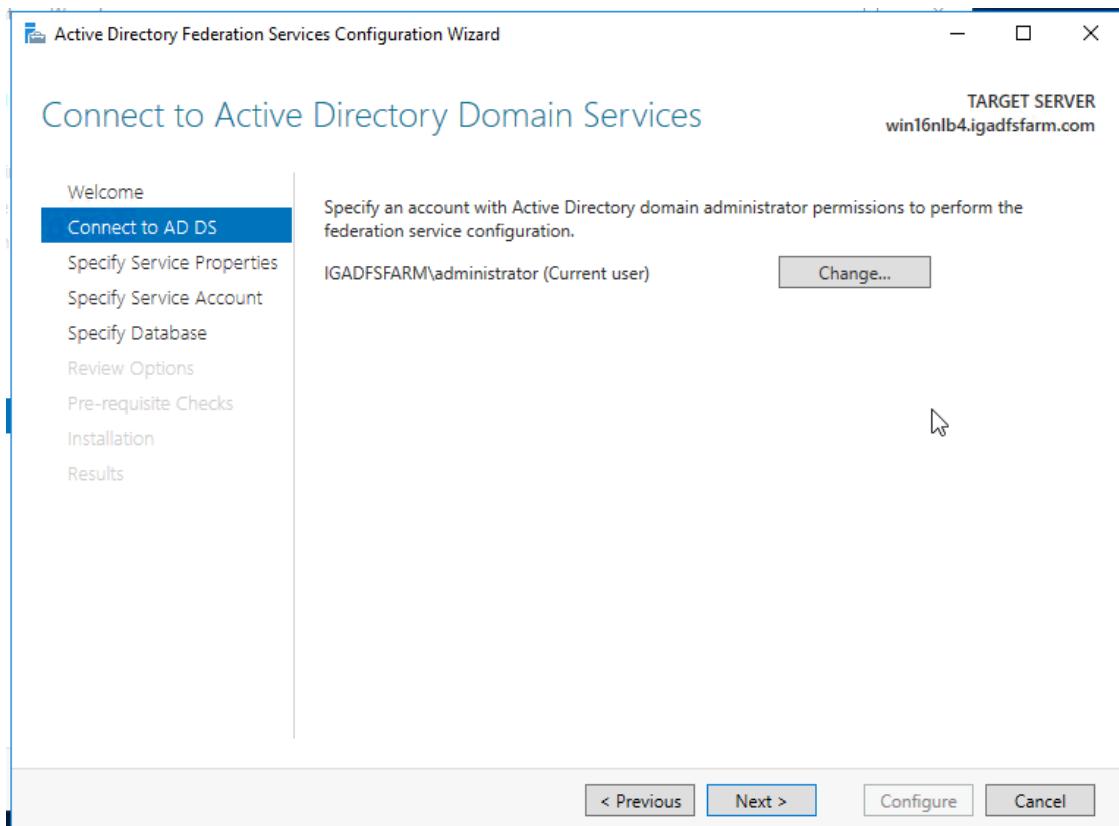
4. Specify the account with administrator permissions and then click **Next**. The **Specify Service Properties** page appears.
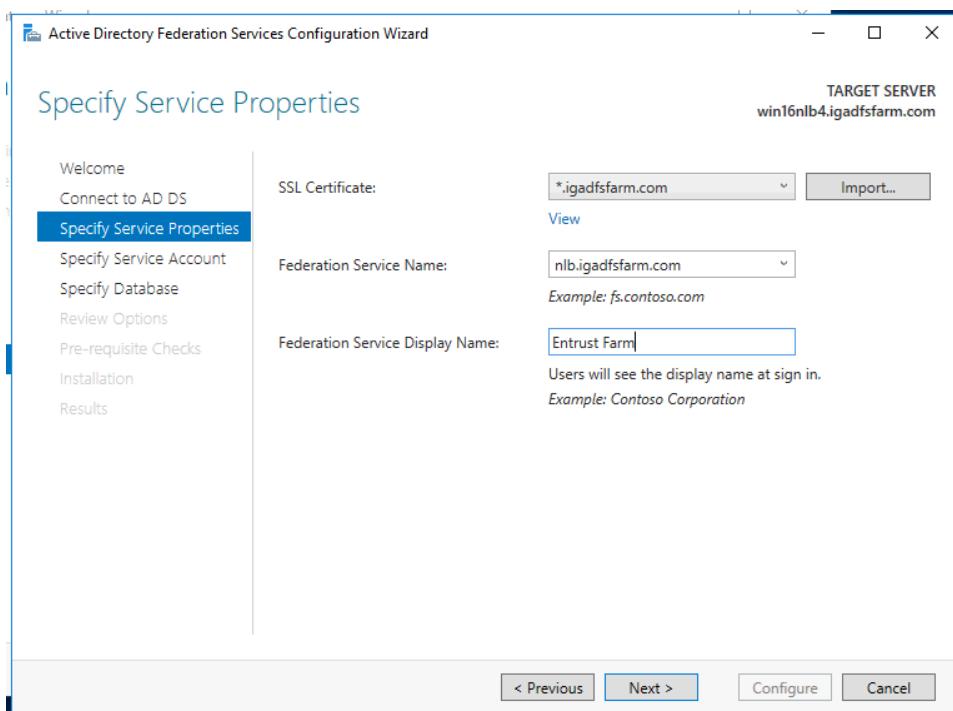

5. On the **Specify Service properties** page, do the following:

    a. Select the SSL certification that you will use.

b. Select the **Federation Service Name**.

c. Enter a **Federation Service Display Name**.

6. Click **Next**. The Specify Service Account page appears.
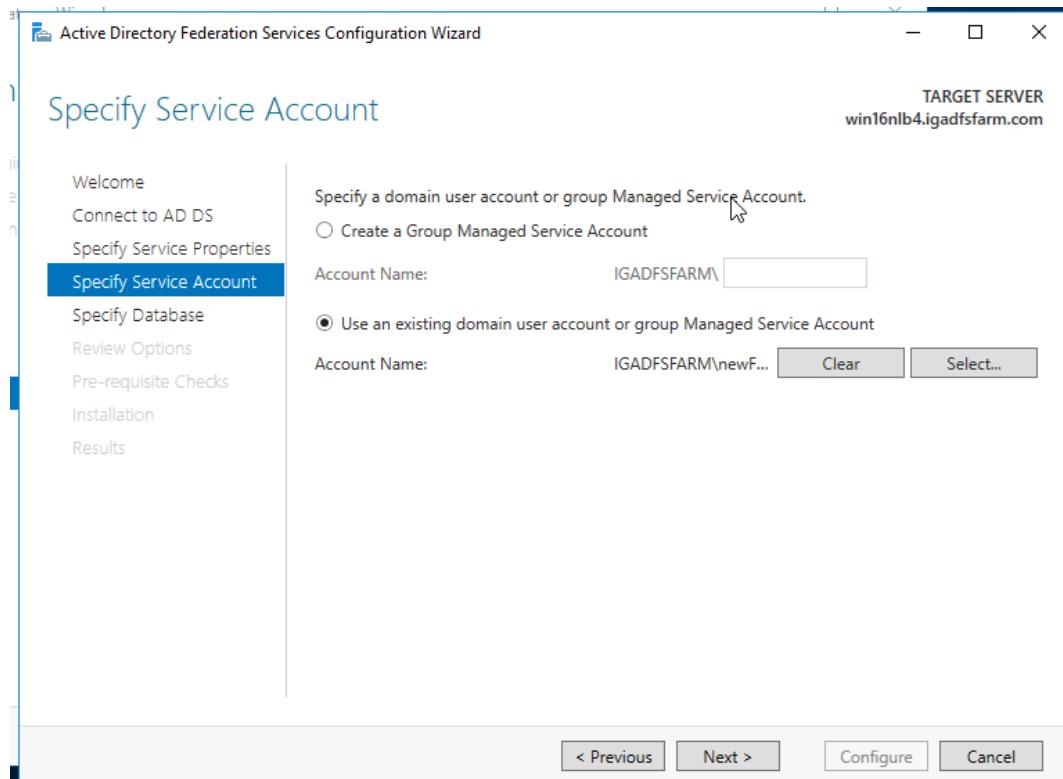
7. Select to either create a Group Managed Service Account or Use an existing Managed Service Account and then click Next. The Specify Configuration Database page appears.
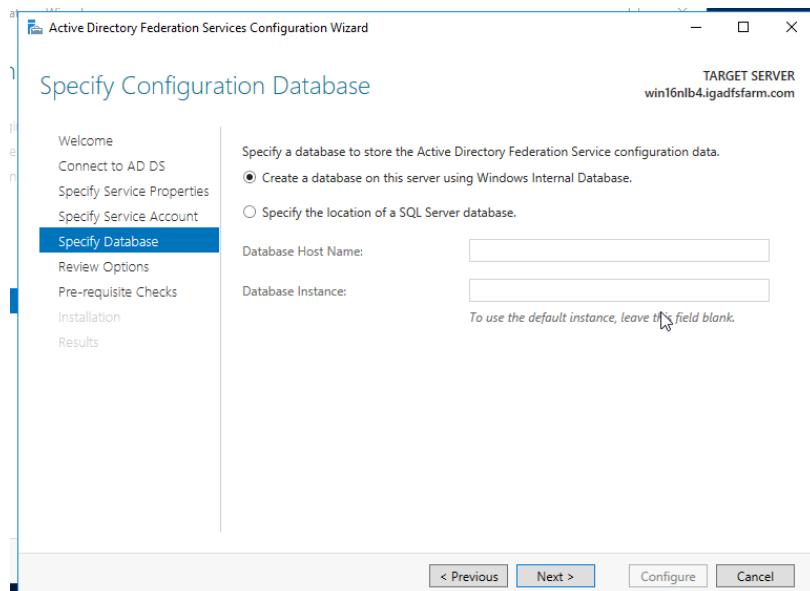
8. Specify an AD FS configuration database by creating a new database or pointing to an existing SQL server and then click **Next**. The **Review Options** page appears.

Active Directory Federation Services Configuration Wizard

Review Options

TARGET SERVER
win16nlb4.igadfsfarm.com

- Welcome
- Connect to AD DS
- Specify Service Properties
- Specify Service Account
- Specify Database
- **Review Options**
- Pre-requisite Checks
- Installation
- Results

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'nlb.igadfsfarm.com'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

A group Managed Service Account IGADFSFARM\newFsGmsa1$ will be created if it does not already exist and this host will be added as a member.

Federation service will be configured to run as IGADFSFARM\newFsGmsa1$.

These settings can be exported to a Windows PowerShell script to automate additional installations

[View script]

[< Previous] [Next >] [Configure] [Cancel]

9. Review your selections and then click **Next**.

10. Click **Configure** and complete the wizard.

Appendix B: Configuring an AD FS sample application

This reference assumes that your environment already has Microsoft OWA, Microsoft SharePoint or any other application you wish to protect configured. Contact Microsoft support if you encounter any issues.

Refer to http://technet.microsoft.com/en-us/library/dn280939.aspx#BKMK_4

Step 3: Configure the Web server (WebServ1) and a sample claims-based application

Step 4: Configure the client computer (Client1)

Installing WAP

WAP is installed using the Roles and Features and by selecting the Remote Services option.

To install WAP on Windows 2012 R2 server

1. Access the **Add Roles and Features** Wizard as follows:

2. To add roles or features by using the Windows interface:

    a. In the **Roles Summary** or **Features Summary** areas of the **Server Manager** main window, click either **Add Roles** or **Add Features**, depending on the software that you want to install.

    b. For WAP select the **Remote Services** option.
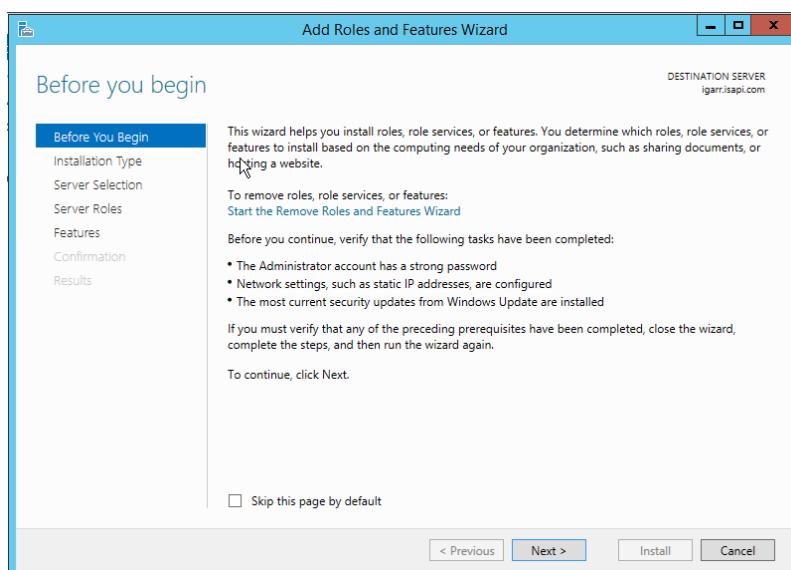
3. Click **Next**. The Installation Type page appears.
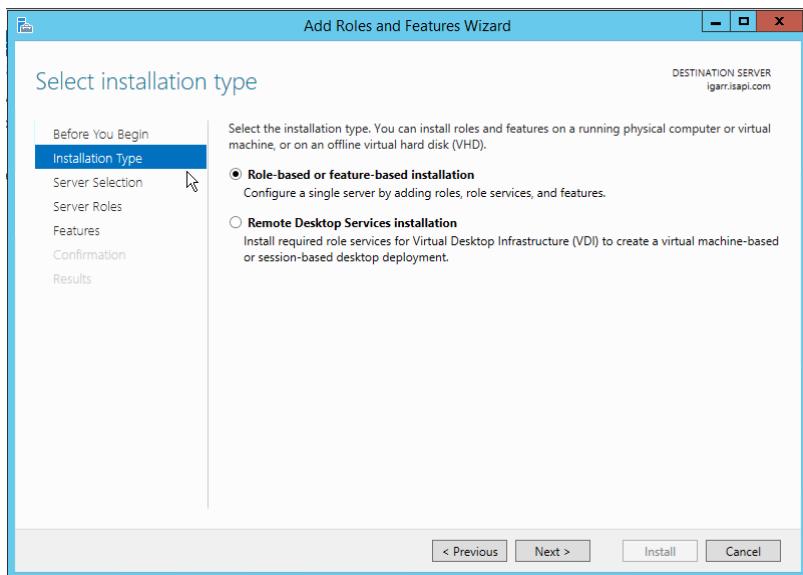
4. Select Role-based or feature-based installation and then click **Next**.

The Server Selection page appears.
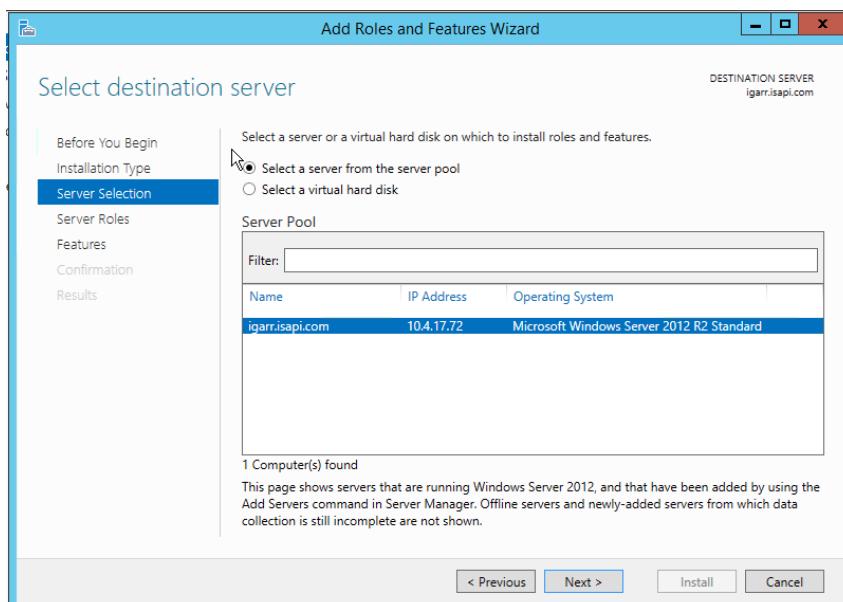
5. Select the server from the **Server Pool** list and then click **Next**.

The Select role services page appears.
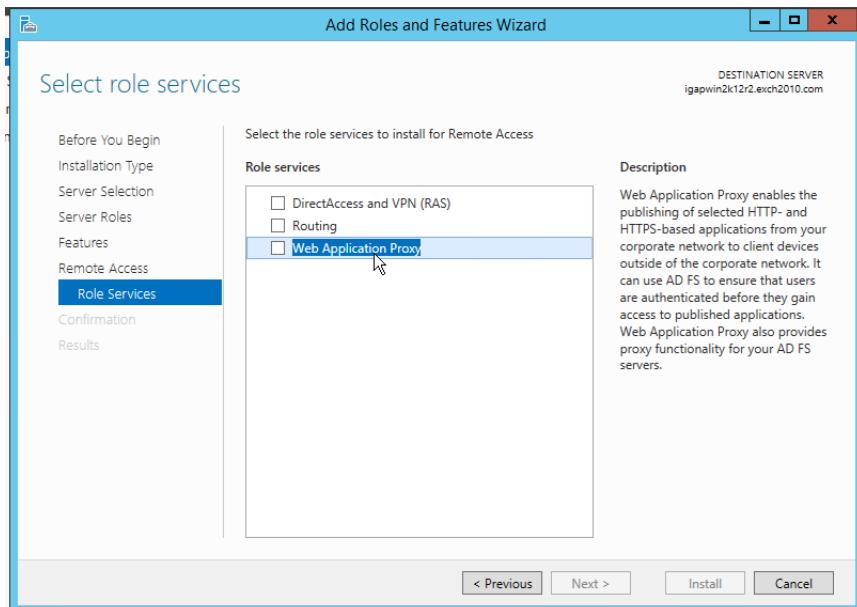
6. Select **Remote Access** and then click **Next** until the Role Services options appears.

7. Select **Web Application Proxy** and then click **Next**.

8. Complete the wizard.

Configuring WAP

To configure WAP

1. Launch the Web Application Proxy Configuration Wizard. To launch the Wizard:

   a. On the Web Application Proxy server, open the Remote Access Management console.

   b. On the Start screen, click the **Apps** arrow.

   c. On the Apps screen, type `RAMgmtUI.exe`, and then press **Enter**.

   d. If the User Account Control dialog box appears, confirm that the action it appears is what you want, and then click **Yes**.

   e. In the navigation pane, click **Web Application Proxy**.

   f. In the Remote Access Management console, in the middle pane, click **Run the Web Application Proxy Configuration Wizard**.

2. Click **Next**. The Federation Server page appears.

3. Choose the AD FS service name that you assigned during the configuration of AD FS and credentials of AD FS:

   a. In the **Federation service name** box, enter the fully qualified domain name (FQDN) of the AD FS server.

   b. In the **User name** and **Password** boxes, enter the credentials of a local administrator account on the AD FS server.

   c. Click **Next**. The AD FS Proxy Certification page appears.

4. Select the certificate for AD FS proxy. The certificate should be the one with the Federation Service name as the subject.

5. Click **Next**. The **Confirmation** page appears.

6. Review the settings on the Confirmation page. If required, you can copy the **PowerShell cmdlet** to automate additional installations.

7. Click **Configure**. The **Results** page appears.

8. In the **Results** page, verify that the configuration was successful and then click **Close**.

# Configuring WAP on Windows server 2016 and 2019

To configure WAP

1. Start the Web Application Proxy Configuration Wizard. To launch the Wizard:

    a. On the Web Application Proxy server, open the Remote Access Management console.

    b. On the Start screen, click the **Apps** arrow.

    c. On the Apps screen, type **RAMgmtUI.exe**, and then press **Enter**.

    d. If the User Account Control dialog box appears, confirm that the action is what you want and then click **Yes**.

    e. In the navigation pane, click **Web Application Proxy**.

    f. In the Remote Access Management console, in the middle pane, click **Run the Web Application Proxy Configuration Wizard**.

2. Click **Next**. The Federation Server page appears.

3. Choose the AD FS service name that you assigned during the configuration of AD FS and credentials of AD FS:

   a. In the **Federation service name** box, enter the fully qualified domain name (FQDN) of the AD FS server.

   b. In the **User name** and **Password** boxes, enter the credentials of a local administrator account on the AD FS server.

   c. Click **Next**. The AD FS Proxy Certification page appears.

4. Select the certificate for the AD FS proxy. The certificate should be the one with the Federation Service name as the subject.

5. Click **Next**. The Confirmation page appears.

6. Review the settings on the Confirmation page. If required, you can copy the **PowerShell cmdlet** to automate additional installations.

7. Click **Configure**. The Results page appears.

8. In the **Results** page, verify that the configuration was successful and then click **Close**.

Publishing AD FS 4.0 and 5.0 sample application on WAP

**To publish AD FS 4.0 and 5.0 sample application on WAP**

1. On the Web Application Proxy Server, access the Remote Access Console.

2. In the Navigation pane, click **Web Application Proxy**.

3. In the **Tasks** pane, click **Publish**. The Publish New Application Wizard appears.
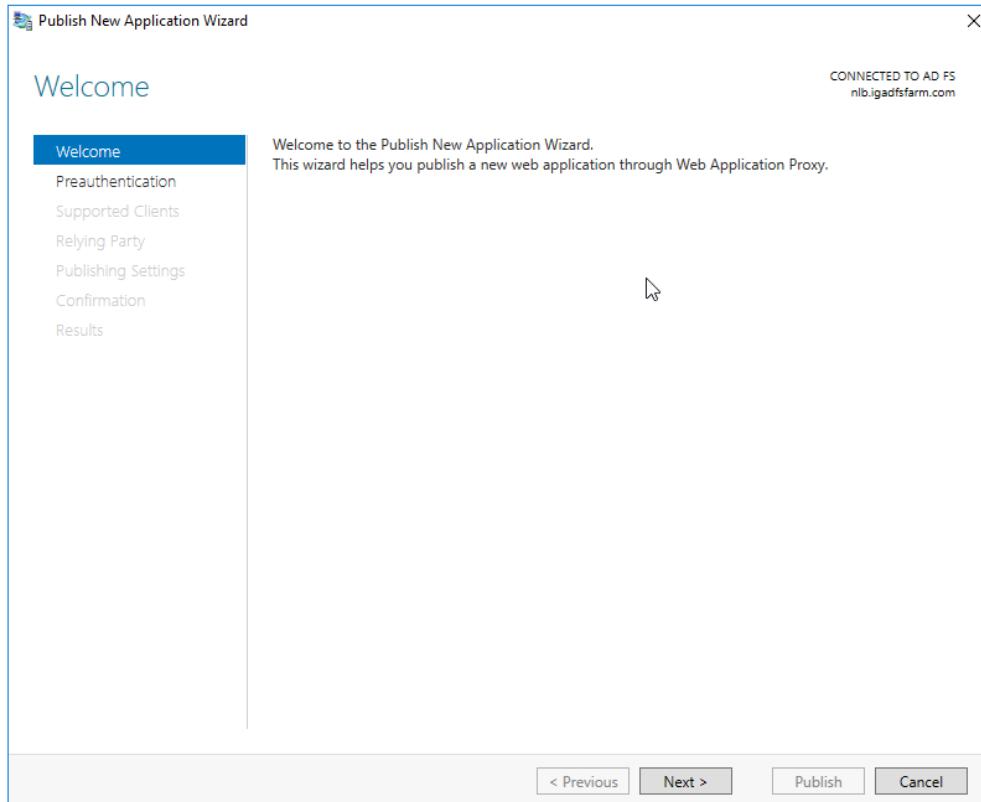
4. On the **Publish New Application Wizard Welcome** page, click **Next**. The Preauthentication page appears.
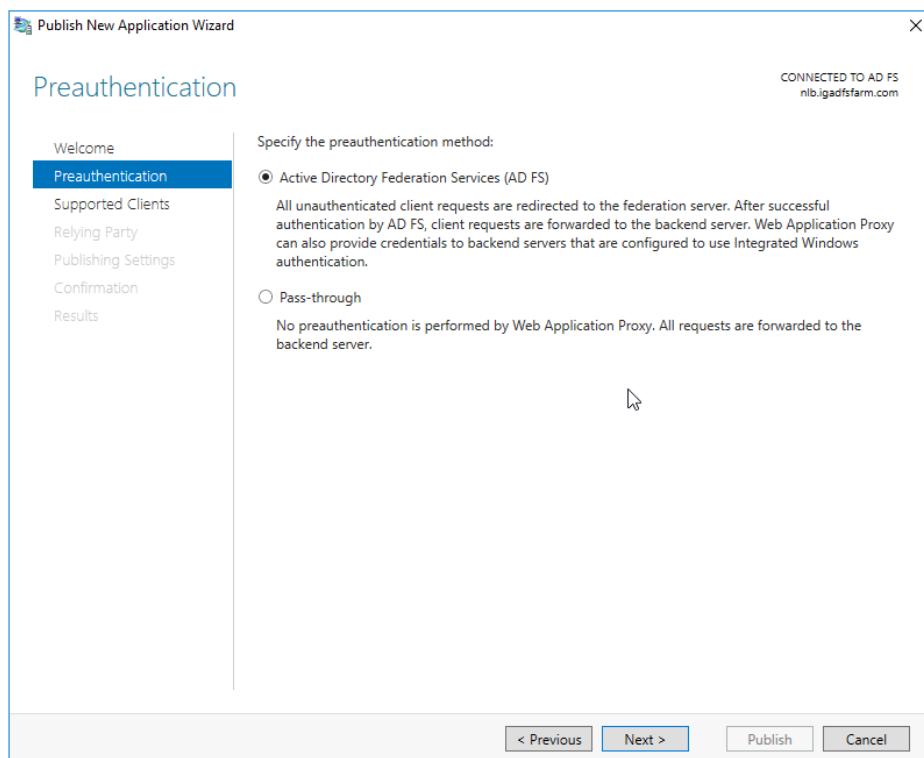
5. Click **Active Directory Federation Services (AD FS)** and then click **Next**. The Relying Party page appears.
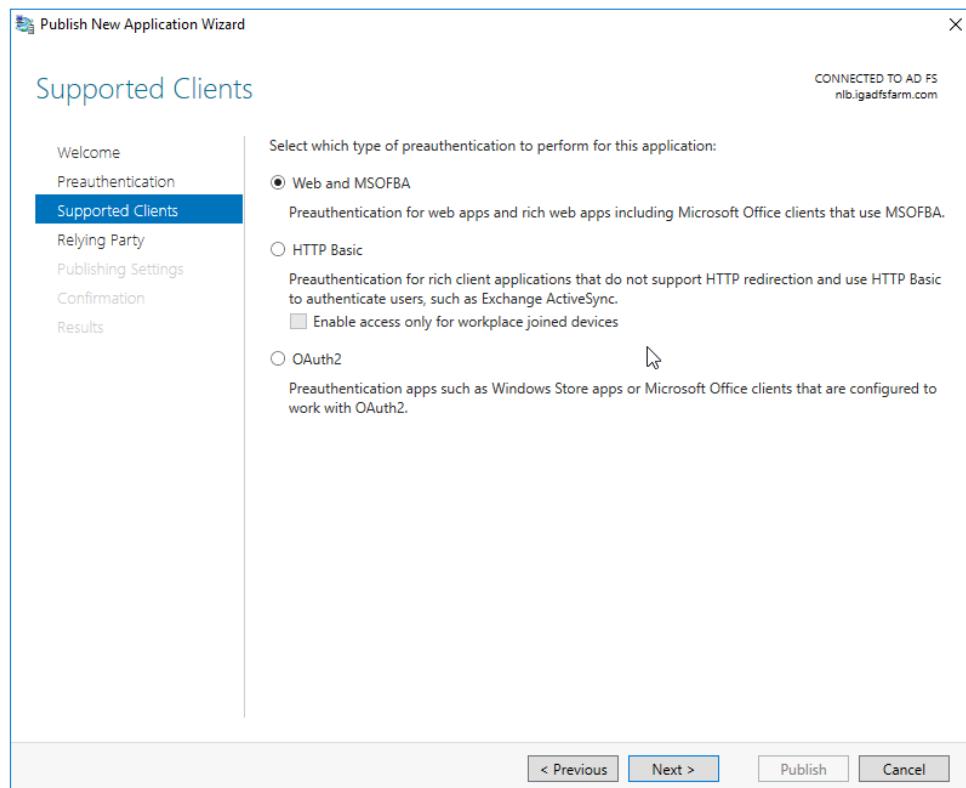
6. For Supported Clients, select **Web and MSOFBA**.
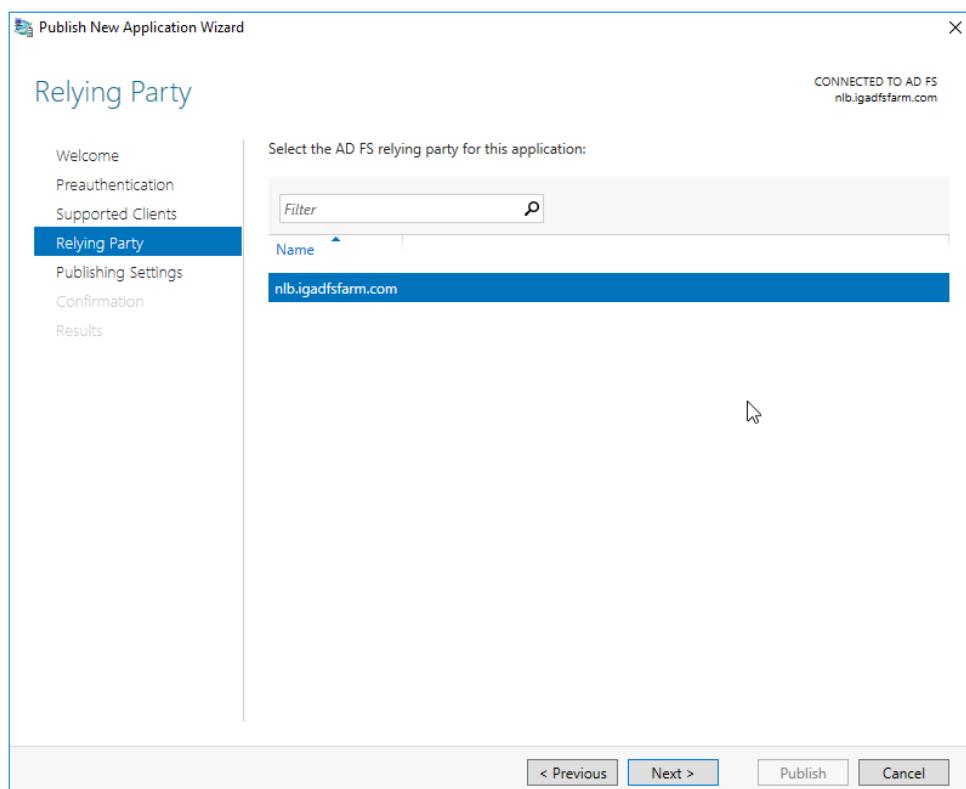
7. In the list of **Relying Parties**, select the Relying Party for the application that you want to publish and then click **Next**.

The Publishing Settings page appears.
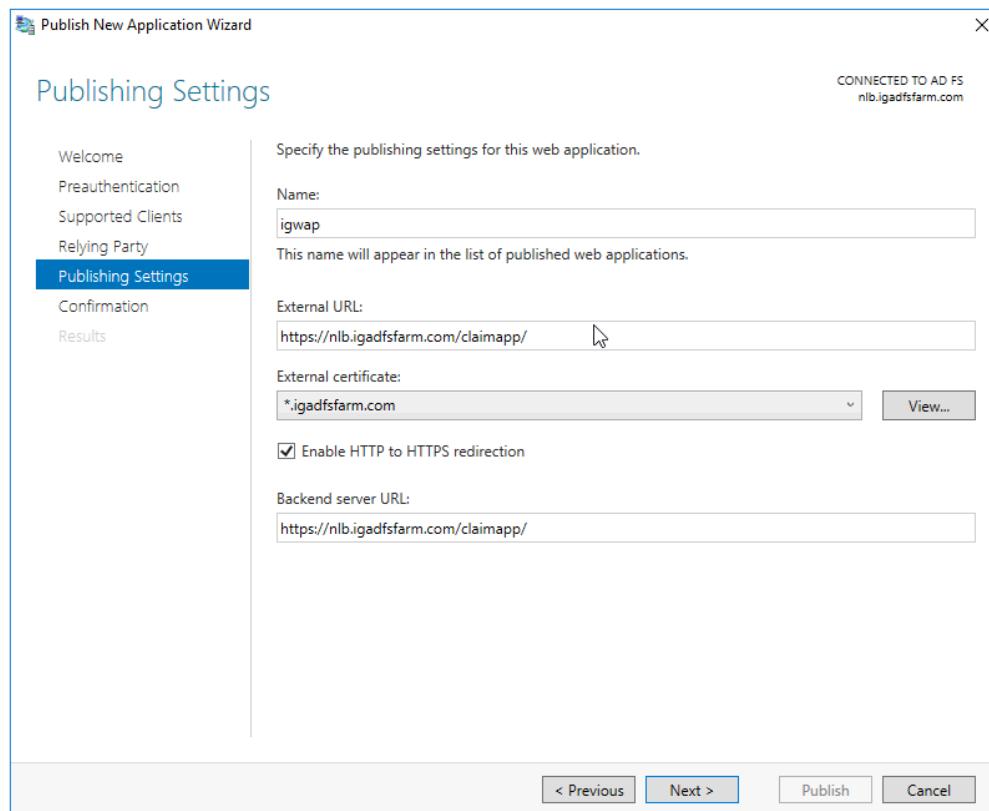
8. On the **Publishing Settings** page, do the following:

   a. In the **Name** box, enter a friendly name for the application.

   This name is used only in the list of published applications in the Remote Access Management console.

   b. In the **External URL** box, enter the external URL for this application.

   c. In the **Backend server URL** box, enter the URL of the backend server. Note that this value is automatically entered when you enter the external URL and you should change it only if the backend server URL is different.

   Note: The Web Application Proxy can translate host names in URLs, but it cannot translate path names. Therefore, you can enter different host names, but you must enter the same path name.

   d. Click **Next**. The Confirmation page appears.
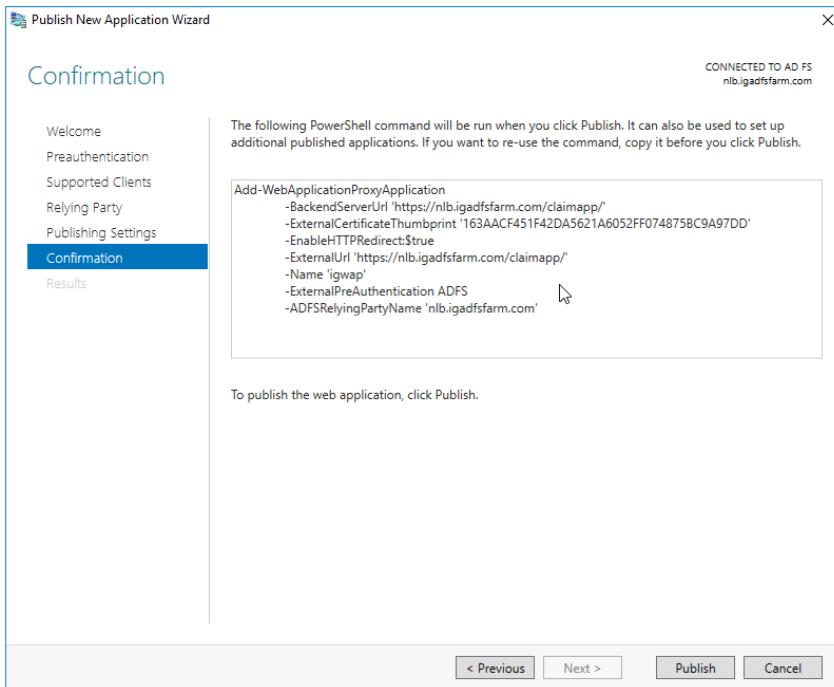
9. Review the settings on the Confirmation page and then click **Publish**. The Results page appears.

Note: If required, you can copy the PowerShell command to set up additional published applications.
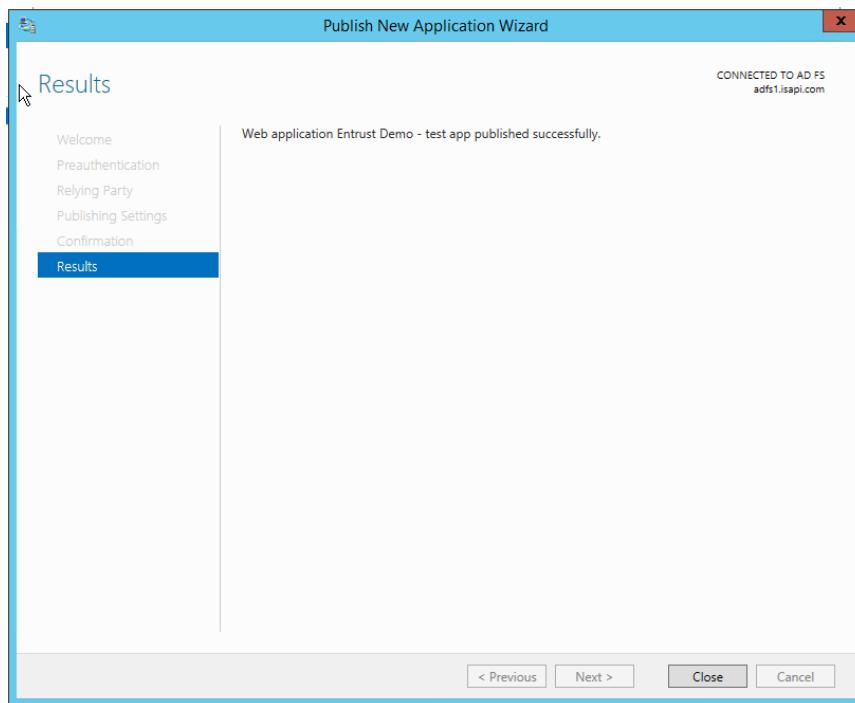
10. On the Results page, make sure the application published successfully and then click **Close**. You are returned to the Remote Access Management Console.

Appendix B: Configuring failover for Entrust Identity Enterprise Servers

You can set up a failover architecture by increasing the number of Entrust Identity Enterprise Servers. With multiple Entrust Identity Enterprise Servers, failover works as follows:

1. Upon startup, the first Entrust Identity Enterprise Server in the list, (also called the preferred server), is used to process all authentication requests.

2. When a successful connection cannot be made to the current, active Entrust Identity Enterprise Server, then the solution fails over to the next available Entrust Identity Enterprise Server, always starting from the preferred server, and skipping over any unavailable servers.

3. At defined intervals that you can configure, the solution attempts to reconnect to the preferred Entrust Identity Enterprise Server. The default interval is one hour.

You can configure failover for Entrust Identity Enterprise Servers by editing the Entrust Identity AD FS Adapter file.

To configure failover for Entrust Identity Enterprise Servers

1. Stop Active Directory Federation Services.

2. Open the file `eigadfsplugin.xml`.

3. Find the IdentityGuardServers element under AuthenticationProvider. For example:

    ```
    <AuthenticationProvider>

           <IdentityGuardServers>

                 ...

           </IdentityGuardServers>

                 ...

    </AuthenticationProvider>
    ```

    Define the attributes of `IdentityGuardServers` as described in the following sub-steps. The attributes defined within this element apply to all the Entrust Identity Enterprise Servers.

    a. Define the `numberOfRetries` attribute. For example:

    ```
    <IdentityGuardServers numberOfRetries="1">
       ...
    </IdentityGuardServers>
    ```

    If the first connection attempt to a server fails, this setting indicates how many further attempts must be made before marking this server as failed. If not specified, the default value is `1`; that is, after an initial (failed) attempt, one further attempt is made.

    b. Define the `delayBetweenRetries` attribute. For example:

    ```
    <IdentityGuardServers numberOfRetries="1"
       delayBetweenRetries="500>
    ...
    </IdentityGuardServers>
    ```

    delayBetweenRetries is used with the numberOfRetries attribute. It specifies how long to wait (in milliseconds) between connection attempts. The default value, if not specified, is 500 milliseconds. If numberOfRetries is 0, then delayBetweenRetries is not used.

    c. Define the `failedServerHoldOffTime` attribute. For example:

```
<IdentityGuardServers numberOfRetries="1"
    delayBetweenRetries="500"
    failedServerHoldOffTime="600">
...
</IdentityGuardServers>
```

failedServerHoldOffTime defines the minimum amount of time (in seconds) that must elapse before attempting to contact a server that has previously been marked as failed. The default value, if not specified, is 600 seconds (10 minutes).

d. Define the `restoreTimeToPreferred` attribute. For example:

```
<IdentityGuardServers numberOfRetries="1"
    delayBetweenRetries="500"
    failedServerHoldOffTime="600"
    restoreTimeToPreferred="3600">
...
</IdentityGuardServers>
```

When the current active, connected server is not the preferred server (that is, the first server in the list), then the restoreTimeToPreferred setting defines how frequently (in seconds) to try to reconnect to the preferred server. The default value, if not specified, is 3600 seconds (one hour). Setting a value of 0 (zero) means that the solution continues to use the current active server, and does not attempt to reconnect to the preferred server.

4. Find the `ServerList` element under `IdentityGuardServers`. For example:

```
<IdentityGuardServers numberOfRetries="1"
      delayBetweenRetries="500"
       restoreTimeToPreferred="3600">
    <ServerList>
    ...
    </ServerList>
</IdentityGuardServers>
```

`ServerList` contains definitions of all the Entrust Identity Enterprise Servers in your environment.

5. Add an `IdentityGuardServer` element under `ServerList`. For example:

6. <ServerList>

```
        <IdentityGuardServer>
                    ...
        </IdentityGuardServer>
</ServerList>
```

Each IdentityGuardServer element defines one of the Entrust Identity Enterprise Servers in your environment.

7. Add an AuthenticationService element under IdentityGuardServer. For example:

```
<ServerList>
     <IdentityGuardServer>
       <AuthenticationService />
     </IdentityGuardServer>
</ServerList>
```

The `AuthenticationService` element contains the URL for the authentication service of the Entrust Identity Enterprise Server being defined.

8. In the `AuthenticationService` element, enter the URL for your first Entrust Identity Enterprise Server. For example:

```
<ServerList>
        <IdentityGuardServer>
          <AuthenticationService
url="https://igserver1.mydomain.com:8443/IdentityGuardAuthService/services/Auth
enticationServiceV12"/>
        </IdentityGuardServer>
</ServerList>
```

This completes the definition of one Entrust Identity Enterprise Server.

9. Repeat steps 4 to 6 for each additional Entrust Identity Enterprise Server in your environment. For example:

```
<ServerList>
        <IdentityGuardServer>
          <AuthenticationService
url="https://igserver1.mydomain.com:8443/IdentityGuardAuthService/services/Auth
enticationServiceV12"/>
        </IdentityGuardServer>

        <IdentityGuardServer>
          <AuthenticationService
url="https://igserver2.mydomain.com:8443/IdentityGuardAuthService/services/Auth
enticationServiceV12"/>
        </IdentityGuardServer>

        <IdentityGuardServer>
          <AuthenticationService
url="https://igserver3.mydomain.com:8443/IdentityGuardAuthService/services/Auth
enticationServiceV12"/>
        </IdentityGuardServer>
</ServerList>
```

10. Save and close `eigadfsplugin.xml`.

11. Restart Active Direction Federation Services for your configuration changes to take effect.

You have completed the configuration of failover for your Entrust Identity Enterprise Servers.