



Technical Integration Guide for Entrust IdentityGuard Adapter 4.0 for Active Directory Federation Services (AD FS) 3.0 and 4.0

Document issue: 1.0

December 2018

Entrust is a trademark or a registered trademark of Entrust Datacard Limited in Canada. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. or Entrust Datacard Limited in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

The information is subject to change as Entrust Datacard reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DATACARD DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST DATACARD SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Copyright © 2018. Entrust Datacard. All rights reserved.

Contents

Introduction	5
Overview Integration information Authentication overview	5 5 6
Two-factor authentication Primary authentication Secondary authentication	8 8 8
Authentication flow Multifactor authentication flow process	8 9
Performing the integration	10
Installing the Entrust IdentityGuard AD FS Adapter	11
Prerequisites Restarting the AD FS service	11 16
Configuring AD FS for Entrust IdentityGuard authentication	17
Testing the integration	
Post-installation configuration	
Configuring the second factor authentication method	24
Configuring policy-based authentication	
Configuring grid authentication	
Configuring token authentication	20 27
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	31 32
Configuring the user domain to Entrust IdentityGuard group mapping	
Migrating users to Entrust IdentityGuard	
Forcing migration	35
Phasing in migration	
Modifying user migration settings	37
Modifying the SkipAuthNoActive element	
Customizing end-user messages	
Configuring logging	
Location of log files	
Changing the log file settings	
Uningthing the Entrust Identity Quard AD ES Adenter	
Uninstalling the Entrust IdentityGuard AD FS Adapter	
Appendix A: Installing and Configuring AD FS 3.0	46
Installing AD FS 3.0	
Configuring AD FS.	
Installing WAP	56 56
Configuring WAP	

http://www.entrustdatacard.com

Publishing AD FS 3.0 sample application on WAP	61
Configuring WAP on Windows server 2016	
Publishing AD FS 4.0 sample application on WAP	
Appendix B: Configuring failover for Entrust IdentityGuard Servers	74
Appendix C: Known issues	

Introduction

This Technical Integration Guide provides an overview of how to integrate Entrust® IdentityGuard Adapter with Mi crosoft® Active Directory Federation Services (AD FS) 3.0 and 4.0. The aim of this integration is to add Entrust IdentityGuard multi-factor authentication (MFA) to AD FS. The Entrust IdentityGuard Adapter uses the pluggable Multi-factor authentication (MFA) option of AD FS to integrate Entrust IdentityGuard MFA with AD FS.

Overview

Entrust IdentityGuard AD FS Adapter integrates the Entrust IdentityGuard Server second factor authentication to Microsoft Active Directory Federation Services.

The Entrust IdentityGuard Server is a server-based software product that authenticates and manages users and their authentication data. Entrust IdentityGuard provides strong second-factor authentication. When AD FS is integrated with the Entrust IdentityGuard AD FS Adapter, the Entrust IdentityGuard 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 IdentityGuard 12.0 FP1 or later

Partner name: Microsoft

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

Product name: Active Directory Federation Services

Product version: 3.0 and 4.0

Partner Product description: In Windows Server® 2012 R2 and Windows Server® 2016, 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 3.0 and 4.0 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

Table 1: Supported authentication methods

Authentication Type	Description
Entrust IdentityGuard 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 IdentityGuard 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 IdentityGuard automatically generates and sends a new supply of OTPs.
	The operation and refresh threshold are defined in Entrust IdentityGuard policy. OTP authentication can be used with a personal verification number (PVN) if your system is set up to require it.
Entrust IdentityGuard 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.
Entrust IdentityGuard 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.
Entrust IdentityGuard Token	In token authentication, the user enters a code generated on a hardware or software token in response to a token challenge. There are two types of hardware tokens:
	response-only (RO)
	challenge-response (CR)
	Token authentication can be used with a personal verification number (PVN) if your system is set up to require it.
Entrust IdentityGuard 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 Entrust IdentityGuard server. A user can accept or reject the challenge, which results in either a successful or failed authentication.
Entrust IdentityGuard 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 IdentityGuard server. A user can accept or reject the challenge, which results in either a successful or failed authentication

Authentication Type	Description
Entrust IdentityGuard Personal Verification Number	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 IdentityGuard 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 IdentityGuard 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.
Entrust IdentityGuard Temporary PIN	A temporary PIN is a fallback authentication method used when the user:
	 is not yet registered for a grid or token the user has last or forgetten their 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.

Two-factor authentication

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

Primary authentication

Windows Server 2012 R2 and Windows Server 2016 supports 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 IdentityGuard.





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 IdentityGuard Multifactor Authentication Adapter.
- 5. Entrust IdentityGuard AD FS Adapter submits the SF challenge page to AD FS and then presents it to the user.
- 6. The user provides SF response to Entrust IdentityGuard Adapter by way of AD FS.
- 7. Entrust IdentityGuard Adapter verifies SF 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

Integrating Active Directory Federation Services and Entrust IdentityGuard Adapter requires that you complete the following steps:

- 1. Install and configure AD FS 3.0 or 4.0.
- **2.** Install and configure WAP.
- 3. Publish an AD FS sample application on WAP.
- 4. Install Entrust IdentityGuard 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 3.0 or 4.0 and at least one Relying Party, protected by AD FS working prior to Entrust IdentityGuard AD FS Adapter integration. Appendix A provides instructions on installing and configuring AD FS 3.0 or 4.0, WAP, and a publishing application. However, it is expected that customers contact Microsoft support if they encounter any issues.

Installing the Entrust IdentityGuard AD FS Adapter

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

Prerequisites

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

- You must install the Entrust IdentityGuard 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 IdentityGuard AD FS Adapter Plugin installer.

To install the Entrust IdentityGuard AD FS Adapter

- 1. Download the Entrust IdentityGuard AD FS Adapter software from Entrust Datacard Trusted Care at https://trustedcare.entrustdatacard.com.
- 2. Copy the software to your computer.
- 3. Double-click the IG ADFS 4.0.msi installer file.

The Entrust IdentityGuard AD FS Adapter Setup Wizard appears.

🖟 Entrust IdentityGuard AD FS Adapter) Setup — 🗆 🗙	(
Welcome to the Entrust IdentityGuard AD FS Adapter 4.0 Setup Wizard	
The Setup Wizard will install Entrust IdentityGuard AD FS Adapter 4.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.	
Back Next Cancel	

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

Entrust IdentityGuard A	D FS Adapter 4	.0 Setup		-)
End-User License Agr	eement					\sim
Please read the followin	g license agreem	ent carefully				×¥
ATTENTION: THIS IS	A LICENSE, I	NOT A SALE	. THIS SOF	TWARE	IS	^
PROVIDED UNDER 1	HE FOLLOWI	NG LICENSE	THAT DEF	INES W	HAT	
YOU MAY DO WITH	THE SOFTWA	RE AND CO	NTAINS LI	MITATI	ONS	
ON REPRESENTATIO	NS, WARRAI	NTIES, CON	DITIONS, R	EMEDI	ES,	
AND LIABILITIES. IF	YOU OBTAIN	IED THIS SO	FTWARE IN	N THE U	NITED	
STATES, "ENTRUST	DATACARD" S	SHALL MEA	N ENTRUST	Γ , INC . Ι	IF YOU	
OBTAINED THIS SOF	TWARE OUT	SIDE OF THE	UNITED S	TATES,		
"ENTRUST DATACA	RD" SHALL M	EAN ENTRU	ST DATACA	ARD LIN	AITED.	
"AFFILIATES" OF EN	TRUST DATA	CARD SHAL	L MEAN AL	L		
CORPORATIONS OF	OTHER ENTI	TIES CONTR	OLLED DIR	ECTLY C	DR	\mathbf{v}
☑ I accept the terms in t	he License Agree	ement				
	Print	Back	Nex	t	Car	ncel

- 6. Read the license agreement for Entrust IdentityGuard software carefully, and select I accept the license agreement.
- 7. Click Next. The Authentication Adapter Setup page appears.

🕼 Entrust IdentityGuard AD FS Adapter 4.0 Setup	-	_	×
Authentication Adapter Setup Enter Application Settings.			
Please enter one or more IdentityGuard servers. Check th IdentityGuard Authentication web service requires an SSL adding more than five servers to the failover pool, consult	e "Requires SSI connection. Fo product docum	" box if the or instructions on entation.	
IdentitvGuard Server	Auth Port	AuthPort Requires SS	L
*			
* - Marks the preferred server.			
Back	Next	Cancel	

- 8. On the Authentication Adapter Setup page, complete the following:
 - **a.** Enter the host names of one or more Entrust IdentityGuard Servers in the **IdentityGuard Server** fields.

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

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

b. Enter the port number being used by the Entrust IdentityGuard 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 IdentityGuard AD FS Adapter.

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

妃 Entrust IdentityGuard AD FS Adapter 4.0 Setup	_		×
Authentication Provider Setup			\sim
Select second-factor authentication type.			
Select authenticator:			
Policy-Based	\sim		
Use Risk-Based Authentication			
Back	lext	Can	cel

- 9. Select the second factor authentication type from the drop-down menu. The default is Policy-based.
 - a. Optionally, select Use Risk-Based Authentication if you want to enable machine authentication.

🕼 Entrust IdentityGuard AD FS Adapter 4.0 Setup	-		×
Cookie Domain			\sim
Enter the cookie domain for IdentityGuard authentication cookies.			
Set the cookie domain to enable single sign-on across multiple hosts.			
Outline Description			
Cookie Domain			
igadfs.com			
Back Next		Cano	ei

10. Click Next. The Cookie Domain page appears.

11. If you are using risk-based authentication, provide the cookie domain for Entrust IdentityGuard authentication cookies.

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

12. Click Next. The Destination Folder page appears.

提 Entrust IdentityGuard AD FS Adapter 4.0 Setup –		×
Destination Folder Click Next to install to the default folder or click Change to choose another.		
Install Entrust IdentityGuard AD FS Adapter 4.0 to:		
Set to cards		_
C:\Program Files\Entrust\IdentityGuard ADFS Adapter\		
Change		
Back Next	Can	cel

- 13. Select the folder where you want to install the application, and click Next.
- 14. The Ready to Install Entrust IdentityGuard AD FS Adapter page appears.



- 15. Click Install to start the installation.
- **16.** The Completed Entrust IdentityGuard AD FS Adapter Setup Wizard page appears.

🖟 Entrust IdentityGuard AD FS	6 Adapter 4.0 Setup — 🗌 🗙			
	Completed the Entrust IdentityGuard AD FS Adapter 4.0 Setup Wizard			
	Click the Finish button to exit the Setup Wizard.			
Please restart your AD FS service.				
	Back Finish Cancel			

17. 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 IdentityGuard authentication

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

This section contains the following procedures:

- To configure AD FS 3.0 for Entrust IdentityGuard Authentication on Windows 2012 R2
- <u>To configure AD FS 4.0 for Entrust IdentityGuard authentication on Windows 2016</u>

To configure AD FS 3.0 for Entrust IdentityGuard Authentication on Windows 2012 R2

- 1. Ensure that you have restarted the Active Directory Federation Services after installing the Entrust IdentityGuard AD FS Adapter (see <u>Restarting the AD FS service</u>).
- 2. Go to Start > Administrative Tools and double-click AD FS Management to open the AD FS Console.

The AD FS Console window appears.

- S	AD FS		_ 🗆 X
훾 File Action View Window Help			_ 8 ×
AD FS	AD FS	Actions	
Point Service Point Service Point Service Authentication Policies	Overview AD FS provides single-sign-on (SSO) access for client computers. Learn More Configuring Trust Relationships Configuring Authentication Policies Troubleshooting AD FS AD FS Help	AD FS Add Relying Party Trust Add Claims Provider Trust Add Attribute Store Edit Federation Service Properties Edit Published Claims Revoke All Proxies View	,
		New Window from Here Refresh Help	

3. Click Authentication Policies. The AD FS Authentication Policies Overview page appears.

\$ 1		AD FS		- D ×
翰 File Action View Window Help				_ <i>6</i> ×
(+ +) 🖄 📰 🖬				
AD FS	Authentication Policies			Actions
Service Trust Relationships	Authentication Policies Ov	erview	^	Authentication Policies
Authentication Policies	You can configure primary authentication and multifactor authentication settings globally or per relying party trust.			Edit Global Primary Authentication Edit Global Multi-factor Authentication
	Learn More			View
	Configuring Authentication Policies			New Window from Here
	AD FS Help		Refresh	
	Primary Authentication			Help
Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.			FS for entication	
	Global Settings			
	Authentication Methods Extranet	Forms Authentication	Edit	
	Device Authentication	Forms Authentication Not enabled		
	Custom Settings		=	
	Per Relying Party		Manage	
	Multi-factor Authentication			
	You can use options below to configure mu device, and location data. Multifactor auth requirements.	ultifactor authentication settings based on us entication is required if there is a match for a	sers/groups, iny of the specified	
	Global Settings			
	Requirements Users/Grou	ps Not configured	Edit	
	Device	Unregistered, Registered		
	Authentication Methods	Not configured		
	Custom Settings	2		
	Per Relying Party		Manage	
			~	
				J.I.

4. Click Edit Global Multi-factor Authentication. The Edit Global Policy Authentication page appears.

Edit Global Authentication Policy
Primary Multi-factor
Configure multi-factor authentication (MFA) settings.
Users/Groups
MFA is required for the following users and groups:
<u>A</u> dd
Remove
Davisas
MFA is required for the following devices:
✓ Unregistered devices
✓ Registered devices
Locations
MFA is required when accessing applications from the following locations:
✓ Extranet
✓ Intranet
Select additional authentication methods. You must select at least one of the following methods to enable MFA:
Certificate Authentication
Entrust IdentityGuard Authentication
What is multifactor authentication?
OK Cancel Apply

- 5. Check Entrust IdentityGuard Authentication to invoke Multi-factor authentication using the Entrust IdentityGuard AD FS Adapter.
- 6. Optional selections:
 - **a.** Under **Users/Groups**, click **Add** to add users or groups that require MFA using the Entrust IdentityGuard AD FS Adapter
 - **b.** Under **Devices**, select **Unregistered Devices**, **Registered Devices**, or both as the triggers to invoke MFA using the Entrust IdentityGuard AD FS Adapter.
 - c. Under Locations, select Extranet, Intranet or both as the triggers to invoke MFA using the Entrust IdentityGuard AD FS Adapter.
- 7. Click OK.

To configure AD FS 4.0 for Entrust IdentityGuard authentication on Windows 2016

- 1. Ensure that you have restarted the Active Directory Federation Services after installing the Entrust IdentityGuard AD FS Adapter (see <u>Restarting the AD FS service</u>).
- 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 Authentication Methods. The AD FS Authentication Methods Overview page appears.



4. Click Edit Multi-factor Authentication Methods. The Edit Authentication Methods appears.

dit Authentication Methods			×
Primary Multi-factor			
Select additional authentication methods. to enable MFA:	You must select at le	east one of the	following methods
Certificate Authentication			
What is multi-factor authentication ?			

- 5. Check Entrust IdentityGuard Authentication to invoke Multi-factor authentication using the Entrust IdentityGuard AD FS Adapter.
- 6. Click OK.

Testing the integration

Before you test your integration, you must create a user in Entrust IdentityGuard and assign a grid 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.

🗲 💿 🥥 https://adfsplugin.adfsig.com/adfs/ls?version=1.0&action=signinℜ 🔎 - 😢 Cetificate error o 🖉 🦉 Sign In	×	
	Entrust IdentityGuard ADFS Adapter	
\times //	Sign in with your organizational account	
	adfsig/adfsuser2	
	Sign in	

The First Factor authentication page appears.

2. Enter your userID and password and click Sign in.

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

🗲 🛞 🖉 https://adfsplugin.adfsig.com/adfs/ls?version=1.08&action=signin&veal 🔎 👻 😒 Cetificate error 🖒 🌈 External Authentication	Me ×
	Entrust IdentityGuard ADFS Adapter
	Welcome ADFSIG\adfsuser2 For security reasons, we require additional information to verify your account
	Entrust IdentityGuard Challenge Authentication To establish your identity, please respond to the followina:
	Please ensure that the serial number on your Entrust IdentityGuard token matches a serial number listed here: 42218-51050 .
	PVN: Update PVN Use temporary PIN
	Submit

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.

E https://adfsplugin.adfsig.com/claimapp/default.aspx	, 𝒫 マ 😵 Certificate error 🖒 🧭 Windows Identity Foundati >	د ا		≙ 🛧
Welcome : ADFSIG/adfsuser2 Values from II.dentity [] [LiAuthenticated True] [Name.ADFSIG adfsuser2] Claims from [ClaimsIdentity				
Claim Type	Claim Value	Value Type	Subject Name	Issuer Name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/implicitupn	adfsuser2@adfsig.com	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	adfsuser2@adfsig.com	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid	S-1-5-21-421438832-262784759-2396311403-513	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid	S-1-5-21-421438832-262784759-2396311403-1603	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ADFSIG\adfsuser2	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname	ADFSIG\adfsuser2	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/claims/authnmethodsreferences	urm: oas is: names: tc: SAML: 2.0: ac: classes: Password Protected Transport Protect	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.com/ws/2012/12/authmethod/identityguard	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.com/claims/multipleauthn	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-21-421438832-262784759-2396311403-513	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus
http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-1-0	string	ADFSIG\adfsuser2	http://adfsplugin.adfsig.com/adfs/services/trus

Post-installation configuration

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

- Configuring the second factor authentication method
- Configuring alternate authenticators
- Configuring the user domain to Entrust IdentityGuard group mapping
- Migrating users to Entrust IdentityGuard
- <u>Customizing end-user messages</u>
- <u>Configuring logging</u>

Configuring the second factor authentication method

After installation you can change the second factor authentication by editing the <code>eigadfsplugin.xml</code> 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 <code>eigadfsplugin.xml</code> 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
- <u>Configuring grid authentication</u>
- <u>Configuring token authentication</u>
- Configuring knowledge-based authentication
- <u>Configuring policy authentication to override Q&A challenge size</u>
- <u>Configuring one-time password (OTP) authentication</u>
- Configuring Mobile Smart Credential authentication (Identity Assured)
- <u>Configuring Mobile Soft Token (TVS) authentication</u>

Configuring policy-based authentication

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

To configure policy-based authentication

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard ADFS Adapter\config and open the eigadfsplugin.xml file.
- 3. Locate the AuthenticationMethods element.

<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 IdentityGuard AD FS Adapter configuration file. Additionally, you can configure grid to specify an enhanced RBA and a particular Entrust IdentityGuard group.

To configure grid authentication

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard 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

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard ADFS Adapter\config and open the eigadfsplugin.xml file.
- 3. Locate the AuthenticationMethods element.

<AuthenticationMethods>

4. 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>
```

- 5. Be sure to uncomment the applicable definition strings.
- 6. Save and close eigadfsplugin.xml.
- 7. Restart Active Directory Federation Services.

Configuring token authentication

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

To configure token authentication

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard ADFS Adapter\config and open the eigadfsplugin.xml file.
- 3. Locate the AuthenticationMethods element.

<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 IdentityGuard 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>\IdentityGuard 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>\IdentityGuard 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"</pre>
cookieName="sequenceNonce" cookieDomain="{cookiedomain}"
cookieLifetime="365" />
                  <UseAppData>false</UseAppData>
            </RegisterMachine>
      </RBA>
</AuthMethod>
```

© Copyright 2018 Entrust Datacard All rights reserved.

- 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>\IdentityGuard 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>
            <Policv>
                <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 IdentityGuard AD FS Adapter configuration file.

To configure OTP authentication

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard 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. 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: IntelliTrust 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 IdentityGuard Server Administration Guide*.

^{7.} Save and close eigadfsplugin.xml.

8. 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 IdentityGuard AD FS Adapter configuration file.

To configure Mobile SC authentication

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard 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 IdentityGuard AD FS Adapter configuration file.

To configure Mobile ST authentication

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard ADFS Adapter\config and open the eigadfsplugin.xml file.

3. Locate the AuthenticationMethods element.

<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"</pre>
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"</pre>
cookieDomain="{cookiedomain}" cookieLifetime="365" />
               <UseSequenceNonce enabled="false"</pre>
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 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 IdentityGuard 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 identityGuard 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

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

External Authentication Method × +	_ 0
🗲 🔒 https://adfs30.adfs.com/adfs/ls/?wa=wsignin1.08vvtrealm=https%3a%2f%2fadfs30.adfs.com%2fclaimapp%2f8vvctx=rm%3d0%26id% 🛡 🤁	Q. Search ☆ 🖻 🖡 🎓 😕
	Entrust IdentityGuard AD FS
	Adapter
	Welcome ADFS\test2
	For security reasons, we require additional information to verify your account
	Entrust IdentityGuard Challenge Authentication
	To establish your identity, please respond to the following:
	Enter a response to the grid challenge [C2] [C5] [11] using a card with serial number: 209
	These are the possible authentication types for this user: Ouestion and Answer
	One-Time Password
	Mobile Soft Token
	l oken Mobile Smart Credential
	Use temporary PIN
	Submit

© Copyright 2018 Entrust Datacard All rights reserved.

To enable alternative authenticators

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard 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:

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 <code>eigadfsplugin.xml</code>.
- 6. Restart Active Directory Federation Services.

Configuring the user domain to Entrust IdentityGuard group mapping

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

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

To configure user domain to Entrust IdentityGuard group mapping

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard ADFS Adapter\config and open the eigadfsplugin.xml file.
- 3. 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 IdentityGuard group is taken as first priority and all other strings are ignored.
- If useDomain is present and if it is false, no Entrust IdentityGuard 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.

- 4. Save and close eigadfsplugin.xml.
- 5. Restart Active Directory Federation Services.

Migrating users to Entrust IdentityGuard

User migration is the process of making all your end users of Entrust IdentityGuard 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 IdentityGuard 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 "<u>Phasing in migration</u>").

To implement forced migration

- 1. Create Entrust IdentityGuard user IDs for all your end users.
- 2. Stop Active Directory Federation Services.
- 3. Go to <adfs_adapter_install>\IdentityGuard 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 IdentityGuard and activate a second-factor authentication method.

Phasing in migration

In this scenario, after you install the Entrust AD FS Adapter, you force all users to enroll with Entrust IdentityGuard 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 IdentityGuard user IDs for your first batch of users.
- 2. Have those users enroll in Entrust IdentityGuard and assign second-factor authentication methods to them.

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

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>\IdentityGuard 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 "<u>Modifying user migration</u>" 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 IdentityGuard, as follows:

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

Users who have already been added in Entrust IdentityGuard 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"></skipauthnoexist>	Non-Entrust IdentityGuard users are blocked from the protected resource. This is the default setting.
<skipauthnoexist enabled="true"></skipauthnoexist>	Non-Entrust IdentityGuard users are allowed access to the protected resource without a second-factor challenge.

If you set	This is the effect
<pre><skipauthnoexist enabled="true" url="IdentityGuardEnrollment.aspx"></skipauthnoexist></pre>	Non-Entrust IdentityGuard 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 IdentityGuard.

Modifying the SkipAuthNoActive element

This element applies to users who have been added to Entrust IdentityGuard, 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"></skipauthnoactive>	Entrust IdentityGuard 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"></skipauthnoactive>	Entrust IdentityGuard 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 <br="" enabled="true">url="IdentityGuardActivation.aspx"/></skipauthnoactive>	Entrust IdentityGuard 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 IdentityGuard AD FS Adapter to meet your regional language requirements.

To customize end-user messages

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard ADFS Adapter\config and open the String.res file.

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

- 3. Edit the messages as required.
- 4. Save and close Strings.res.
- 5. Restart Active Directory Federation Services.

Configuring logging

You can configure logging for the Entrust IdentityGuard AD FS Adapter independently. The Entrust IdentityGuard AD FS Adapter uses Apache logging packages to implement logging. The Entrust IdentityGuard 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\IdentityGuard ADFS Adapter\log.

Changing the logging level

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

The default logging level for the Entrust IdentityGuard 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 IdentityGuard AD FS Adapter logging level

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard 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 IdentityGuard AD FS Adapter

- 1. Stop Active Directory Federation Services.
- 2. Go to <adfs_adapter_install>\IdentityGuard 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\IdentityGuard 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.

Uninstalling the Entrust IdentityGuard AD FS Adapter

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

This section contains the following procedures:

- To uninstall the Entrust IdentityGuard AD FS Adapter on Windows server 2012 R2
- To uninstall the Entrust IdentityGuard AD FS Adapter on Windows server 2016

To uninstall the Entrust IdentityGuard AD FS Adapter on Windows server 2012 R2

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

The Edit Global Policy Authentication page appears.

Edit Global Authentication Policy
Primary Multi-factor
Configure multi-factor authentication (MFA) settings.
Users/Groups MFA is required for the following users and groups:
Add Remove
Devices
MFA is required for the following devices:
✓ Unregistered devices
✓ Registered devices
Locations
MFA is required when accessing applications from the following locations:
✓ Extranet
✓ Intranet
Select additional authentication methods. You must select at least one of the following methods to enable MFA:
Certificate Authentication
Entrust IdentityGuard Authentication
What is multifactor authentication?
OK Cancel Apply

- 2. Uncheck Entrust IdentityGuard Authentication and then click OK.
- 3. Go to Control Panel > Programs > Uninstall a program and double-click Entrust IdentityGuard AD FS Adapter. The AD FS Setup wizard opens.

To uninstall the Entrust IdentityGuard AD FS Adapter on Windows server 2016

1. Go to the AD FS console and select Service > Authentication Methods > Edit Multi-factor Authentication Methods.

The Edit Authentication Methods page appears.

Edit Aut	hentication	Methods				×
Primary	Multi-factor					
Select a to enab	additional auth ble MFA:	hentication meth	iods. You mu	ist select at lea	ast one of the fo	ollowing methods
Cer	tificate Auther ıre MFA	ntication	t			
	rust identityGi	uard Authenticat	ion			
What is	s multi-factor a	authentication?				
				ОК	Cancel	Apply

- 2. Uncheck Entrust IdentityGuard Authentication and then click OK.
- 3. Go to Control Panel > Programs > Uninstall a program and double-click Entrust IdentityGuard AD FS Adapter.

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



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

-OR-

Double-click the $IG_ADFS_4.0.msi$ installer file. The Entrust IdentityGuard AD FS Adapter Setup Wizard appears.

🥵 Entrust IdentityGuard AD FS	Adapter 4.0 Setup – 🗆 🗙
	Welcome to the Entrust IdentityGuard AD FS Adapter 4.0 Setup Wizard
	The Setup Wizard allows you to change the way Entrust IdentityGuard AD FS Adapter 4.0 features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel

5. Click Next. The Change, Repair, or Remove Installation page appears.

🕼 Entrust IdentityGuard AD FS Adapter 4.0 Setup -	×
Change, repair, or remove installation Select the operation you wish to perform.	
Change Entrust IdentityGuard AD FS Adapter 4.0 has no independently selectable features. Repair Entrust IdentityGuard AD FS Adapter 4.0 cannot be repaired.	
Remove Removes Entrust IdentityGuard AD FS Adapter 4.0 from your computer.	
Back Next Can	cel

6. Click Remove.

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

Warning	
lf you have not already done so, uncheck "Entrust IdentityGuard Authentication" Plugin from:	
AD FS -> Edit Global Authentication Policy	
You must do this before clicking "OK" on this dialog.	
ОК	

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

Appendix A: Installing and Configuring AD FS 3.0

This Appendix provides instructions on installing and configuring AD FS 3.0, WAP and a publishing application. However, it is expected that customers contact Microsoft support if they encounter any issues.

Installing AD FS 3.0

You can install AD FS 3.0 using the Roles and Features and select Active Directory Federation services.

To install AD FS 3.0

1. 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 to access the Add Roles and Features Wizard.



- 2. Click Next. The Select installation type page appears.
- **3.** Select Role-based or feature-based installation and then click **Next**. The Select Destination Server page appears.

Select destinat	ion server			DESTINATION SERVE igarr.isapi.co
Before You Begin Installation Type Server Selection Server Roles	Select a server or Select a server Select a virtual Server Pool	a virtual hard disk on whic from the server pool hard disk	h to install roles and features.	
Features Confirmation	Filter:			
	Name	IP Address	Operating System	
	igarr.isapi.com	10.4.17.72	Microsoft Windows Server 20	12 R2 Standard
	1 Computer(s) fou This page shows s Add Servers comm collection is still in	nd ervers that are running Wi 1and in Server Manager. C complete are not shown.	ndows Server 2012, and that have ffline servers and newly-added se	been added by using t rvers from which data

4. Select the server and then click **Next**. The Select Server Roles page appears.

à .	Add Roles and Features Wizard	_ □ ×
Select server roles Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DHCP Server DHCP Server Fax Server	DESTINATION SERVER igar:ispl.com Description Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.
	File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access (1 of 3 installed) Remote Desktop Services V	t > Install Cancel

5. Select Active Directory Federation Services, click Next and then click Complete the wizard.

Configuring AD FS

The next step is to configure Active Directory Federation Services.

This section includes the following topics:

- <u>To configure AD FS 3.0</u>
- <u>To configure AD FS 4.0</u>

To configure AD FS 3.0

- 1. Start the AD FS configuration wizard from the server manager. The AD FS Configuration Wizard appears.
- **2.** There are two ways to start the AD FS Federation Server Configuration Wizard. To start the wizard, do one of 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.
 - **b.** Any time after the setup wizard is complete, open Windows Explorer, navigate to the C:\Windows\AD FS folder, and then double-click **FsConfigWizard.exe**.

È.	Active Directory Federation Services Configuration Wizard
Welcome	TARGET SERVER igwin2012r2adfs.isapi.com
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Confirm Overwrite Review Options Pre-requisite Checks Installation Results	 Welcome to the Active Directory Federation Services Configuration Wizard. Before you begin configuration, you must have the following: An Active Directory domain administrator account. A publicly trusted certificate for SSL server authentication. AD FS pre-requisites Select an option below: Create the first federation server in a federation server farm Add a federation server to a federation server farm
	< Previous Next > Configure Cancel

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.

<u>ل</u>	ctive Directory Federation Services Configuration Wizard
Connect to Active	e Directory Domain Services Igwin2012r2adfs.isapi.com
Welcome Connect to AD DS	Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.
Specify Service Properties Specify Service Account Specify Database	ISAPI\Administrator (Current user) Change
Confirm Overwrite Review Options	
Pre-requisite Checks Installation	
resurs	
	< Previous Next > Configure Cancel

 Specify the account with administrator permissions and then click Next. The Specify Service Properties page appears.

ia 1	Active Directory Federation Servic	es Configuration Wizard	_ 🗆 X	
Specify Service P	roperties		TARGET SERVER igwin2012r2adfs.isapi.com	
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	mail.isapi.com View	▼ Import	
Specify Service Account Specify Database	Federation Service Name:	adfs1.isapi.com Example: fs.contoso.com	•	
Review Options Pre-requisite Checks	Federation Service Display Name:	Entrust Demo Users will see the display name	e at sign in.	
Installation Results		Example: Contoso Corporation		
< Previous Next > Configure Cancel				

- 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.

<u>م</u>	Active Directory Federati	on Services Configuration Wiz	ard 💶 🗖 🗙
Specify Service A	ccount		TARGET SERVER igwin2012r2adfs.isapi.com
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database	Specify a domain user acc Create a Group Manag Account Name: Use an existing domai	ount or group Managed Service Acco ged Service Account ISAPN n user account or oroup Managed Ser	unt.
Confirm Overwrite Review Options Pre-requisite Checks Installation Results	G Ose an existing domain	ISAPI\adfs3\$	Clear Select
		< Previous Next >	Configure Cancel

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.

<u>م</u>	Active Directory Federation Services	Configuration Wizard	- 🗆 X
Specify Configura	tion Database	T igwin2012ri	ARGET SERVER 2adfs.isapi.com
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Confirm Overwrite	Specify a database to store the Active D © Create a database on this server usin O Specify the location of a SQL Server Database Host Name:	rectory Federation Service configuration dat g Windows Internal Database. database.	а.
Review Options Pre-requisite Checks Installation Results	Database Instance:	To use the default instance, leave this field b	lank.
< Previous Next > Configure Cancel			

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.

A A	ctive Directory Federation Services Configuration Wizard
Review Options	TARGET SERVER igwin2012r2adfs.isapi.com
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Confirm Overwrite 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 'adfs1.isapi.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. All existing configuration in the database will be deleted. A group Managed Service Account ISAPI\adfs3\$ 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 ISAPI\adfs3\$.
	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.

To configure AD FS 4.0

- 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.



© Copyright 2018 Entrust Datacard All rights reserved.

http://www.entrustdatacard.com

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.

Active Directory Federation Serv	ices Configuration Wizard	- 🗆 ×
Connect to Active	Directory Domain Services	TARGET SERVER win16nlb4.igadfsfarm.com
Welcome Connect to AD DS	Specify an account with Active Directory domain administrator pe federation service configuration.	rmissions to perform the
Specify Service Properties Specify Service Account Specify Database	IGADFSFARM\administrator (Current user)	hange
Review Options Pre-requisite Checks Installation		ß
Results		
	< Previous Next >	Configure Cancel

4. Specify the account with administrator permissions and then click **Next**.

The Specify Service Properties page appears.

Active Directory Federation Ser	vices Configuration Wizard	- 🗆 X
Specify Service Pr	operties	TARGET SERVER win16nlb4.igadfsfarm.com
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	*igadfsfarm.com v Import
Specify Service Account Specify Database Review Options	Federation Service Name:	nlb.igadfsfarm.com v Example: fs.contoso.com
Pre-requisite Checks Installation Results	Federation Service Display Name:	Entrust Farm Users will see the display name at sign in. <i>Example: Contoso Corporation</i>
		Previous Next > Configure Cancel

- 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.

at	Active Directory Federation Serv	ices Configuration Wizard		-	-		×
ı	Specify Service Ad	count		win16nlb	TAR 4.igad	GET SEF	COM COM
jii e n	Welcome Connect to AD DS Specify Service Properties Specify Service Account	Specify a domain user a O Create a Group Mar Account Name:	account or group Managed Service Account. naged Service Account IGADFSFARM\				
	Specify Database	 Use an existing dom 	nain user account or group Managed Service A	Account			
	Review Options Pre-requisite Checks	Account Name:	IGADFSFARM\newF	Clear	S	elect	
	Installation						
Ĩ							
			< Previous Next >	Configure		Cance	9

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.

at	Active Directory Federation Sen	vices Configuration Wizard	/	_		×
n	Specify Configura	tion Database		TAI win16nlb4.iga	RGET SEF adfsfarm.	RVER .com
pil n	Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Specify a database to store the Actin © Create a database on this server O Specify the location of a SQL Ser Database Host Name: Database Instance:	e Directory Federation Service con using Windows Internal Database. ver database.	figuration data.	nk.	
			< Previous Next >	Configure	Cance	el 🛛

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 Servi	ces Configuration Wizard	_		×
F	eview Options		T/ win16nlb4.iq	ARGET SE gadfsfarm	RVER .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 farr AD FS configuration will be stored in Windows Internal Database. Windows Internal Database feature will be installed on this server if it i A group Managed Service Account IGADFSFARM\newFsGmsa1\$ will be already exist and this host will be added as a member. Federation service will be configured to run as IGADFSFARM\newFsGm These settings can be exported to a Windows PowerShell script to auto additional installations	m 'nlb.igadfsfa s not already e created if it i isa1\$.	rm.com'. installed. does not	vt
		< Previous Next >	Configure	Cance	el

- 9. Review your selections and then click **Next**.
- **10.** Click **Configure** and complete the wizard.

Configuring an AD FS 3.0 and 4.0 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.

b	Add Roles and Features Wizard
Before you begin Before You Begin Installation Type Server Roles Features Confirmation Results	Add Roles and Features Wizard
	If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again. To continue, click Next. Skip this page by default Previous Next > Install Cancel

3. Click Next. The Installation Type page appears.

b	Add Roles and Features Wizard
Select installat Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Image: Stratton Stryck Igan: Ig
	< Previous Next > Install Cancel

4. Select Role-based or feature-based installation and then click Next.

The Server Selection page appears.

b	Add Roles and Features Wizard
Select destinatio	N SETVER
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool
Confirmation	Filter:
(Legisland	igarr.isapi.com 10.4.17.72 Microsoft Windows Server 2012 R2 Standard 1 Computer(s) found
	This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown. < Previous Next > Install Cancel

5. Select the server from the $\ensuremath{\mathsf{Server}}\xspace{\mathsf{Pool}}$ list and then click $\ensuremath{\mathsf{Next}}\xspace.$

The Select role services page appears.

Select role serv	ICES Select the role services to install for Remote Access	DESTINATION SERVER igapwin2k12r2.exch2010.com
Installation Type Server Selection Server Roles Features Remote Access Role Services Confirmation Results	Role services DirectAccess and VPN (RAS) Routing Web Application Proxy	Description Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from you corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provide proxy functionality for your AD FS servers.

- 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**.

Welcome	DESTINATION SERVER igwap.isapi.com
Welcome Federation Server AD FS Proxy Certificate Confirmation Results	Web Application Proxy is a Remote Access service used to publish web applications that end users can interact with from any device. It also provides proxy functionality for Active Directory Federation Services (AD FS) to help system administrators provide secure access to an AD FS server. By using Web Application Proxy, system administrators can choose how end users should authenticate themselves to a web application and which users are authorized to use a web application.
	ŀ₹

2. Click Next. The Federation Server page appears.

학	Web Application Proxy Configuration Wizard
Federation Serve	C DESTINATION SERVER
Welcome Federation Server	Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization.
AD FS Proxy Certificate	Federation service name:
Confirmation	igadfs.isapi.com
	Enter the credentials of a local administrator account on the federation servers. User name: administrator
	Password:
	••••••
	< Previous Next > Configure Cancel

- 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.

\$j	Web Application Proxy Configuration Wizard	x
AD FS Proxy Cert	ificate	STINATION SERVER igwap.isapi.com
Welcome Federation Server AD F5 Proxy Certificate Confirmation Results	Select a certificate to be used by the AD FS proxy:	View
	< Previous Next > Configure	Cancel

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**.

Publishing AD FS 3.0 sample application on WAP

To publish AD FS 3.0 sample application on WAP

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

對		Remote Access I	Management Console		_ 0
Via Configuration Web Application Proxy	PUBLISHED WEB APPLICA All published web applications	TIONS 3 total			> Tasks General
Operations Status	Filter	۹		۲	Publish Refresh claimapp
∎ igarr	Name	External URL	Backend Server URL	Preauthentication	Remove Publish based on this application

- 2. In the Navigation pane, click Web Application Proxy.
- 3. In the Tasks pane, click Publish. The Publish New Application Wizard appears.

载	Publish New Application Wizard	x
Welcome		CONNECTED TO AD FS adfs1.isapi.com
Welcome Preauthentication Relying Party Publishing Settings Confirmation Results	Welcome to the Publish New Application Wizard. This wizard helps you publish a new web application through Web Application Proxy.	
	< Previous Next > Public	sh Cancel

4. On the **Publish New Application Wizard Welcome** page, click **Next**. The Preauthentication page appears.

S i	Publish New Application Wizard
l&reauthentication	CONNECTED TO AD FS adfs1.isapi.com
Welcome	Specify the preauthentication method:
Preauthentication	Active Directory Federation Services (AD FS)
Relying Party Publishing Settings Confirmation Results	All unauthenticated client requests are redirected to the federation server. After successful authentication by AD FS, client requests are forwarded to the backend server. Web Application Proxy can also provide credentials to backend servers that are configured to use Integrated Windows authentication. Pass-through No preauthentication is performed by Web Application Proxy. All requests are forwarded to the backend server.
	< Previous Next > Publish Cancel

- 5. Click Active Directory Federation Services (AD FS) and then click Next. The Relying Party page appears.
- 6. 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.

载	Publish New Application Wizard	:
Publishing Setting	S CONNECTED TO AD FS adds1.lispl.com	
Welcome Preauthentication Relying Party Publishing Settings Confirmation Results	Specify the publishing settings for this web application. Name: Entrust Demo - test app This name will appear in the list of published web applications. External URL: https://adfs1.isapi.com/webclaim/ External certificate: adfs1.isapi.com View Backend server URL: https://adfs1.isapi.com/webclaim/	
	< Previous Next > Publish Cancel	

7. On the **Publishing Settings** page

- **a.** In the **Name** box, enter a friendly name for the application.
- **b.** This name is used only in the list of published applications in the Remote Access Management console.
- c. In the External URL box, enter the external URL for this application.
- d. 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.
- e. Note: Web Application Proxy can translate host names in URLs, but cannot translate path names. Therefore, you can enter different host names, but you must enter the same path name.
- f. Click Next. The Confirmation page appears.

5	Publish New Application Wizard	x
Confirmation	CONNECTED TO AD FS adfs1.isapi.com	
Welcome Preauthentication Relying Party Publishing Settings Confirmation Results	The following PowerShell command will be run when you click Publish. It can also be used to set up additional published applications. If you want to re-use the command, copy it before you click Publish. Add-WebApplicationProxyApplication -BackendServerUrl 'Inttps://adf31.isapi.com/webclaim/' -ExternalUrl'https://adf31.isapi.com/webclaim/' -Name 'Entrust Demo - test app' -ExternalPreAuthentication ADFS -ADFSRelyingPartyName 'webclaim' To publish the web application, click Publish.	
	< Previous Next > Publish Cancel]

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.

朝	Publish New Application Wizard
Results	CONNECTED TO AD FS adfs1.isapi.com
Welcome Preauthentication Relying Party Publishing Settings Confirmation Results	Web application Entrust Demo - test app published successfully.
	< Previous Next > Close Cancel

9. On the Results page, make sure the application published successfully and then click **Close**. You are returned to the Remote Access Management Console.

To install WAP on Windows 2016 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.

📥 Add Roles and Features Wi	zard	-		×
Select installation	on type	DESTIN igwap.i	ATION SER gadfsfarm.c	/ER iom
Before You Begin Installation Type Server Roles Features Remote Access Role Services Confirmation Results	Select the installation type. You can install roles and features on a running physi machine, or on an offline virtual hard disk (VHD). © Role-based or feature-based installation Configure a single server by adding roles, role services, and features. © Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create or session-based desktop deployment.	a virtual m	ter or virt	ual ased
	< Previous Next >	nstall	Cance	el

4. Select Role-based or feature-based installation and then click Next.

The Server Selection page appears.

Add Roles and Features Wiza	ra			_		^
Select destinatio	on server			DESTIN ígwap.i	ATION SER gadfsfarm.o	COM
Before You Begin Installation Type	Select a server or a virtual Select a server from th	hard disk on which t e server pool	o install roles and features.			
Server Selection Server Roles Features	Server Pool	sk				
Remote Access	Filter:					
Role Services	Name	IP Address	Operating System			
	igwap.igadfsfarm.com	10.4.18.17,10.4	Microsoft Windows Server	2016 Standard		
	1 Computer(s) found This page shows servers th and that have been added newly-added servers from	hat are running Wind I by using the Add Se which data collectio	lows Server 2012 or a newer r ervers command in Server Ma n is still incomplete are not sl	release of Wind mager. Offline : hown.	lows Serv servers ar	ver, nd

5. Click Select a server from the server pool and then click Next.

The Select role services page appears.

À	Add Roles and Features Wizard	_ _ ×
Select role service	es	DESTINATION SERVER igapwin2k12r2.exch2010.com
Before You Begin Installation Type Server Selection Server Roles Features Remote Access Role Services Confirmation Results	Select the role services to install for Remote Access Role services DirectAccess and VPN (RAS) Routing Web Application Proxy	Description Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.
	< Previous N	ext > Install Cancel

- 6. Select Remote Access > Role Services.
- 7. Select Web Application Proxy and then click Next.
- 8. Complete the wizard.

Configuring WAP on Windows server 2016

To configure WAP

- 9. 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**.

Sa Web Application Proxy Configur	ration Wizard X
Welcome	DESTINATION SERVER igwap.igadfsfarm.com
Welcome Federation Server AD FS Proxy Certificate Confirmation Results	Web Application Proxy is a Remote Access service used to publish web applications that end users can interact with from any device. It also provides proxy functionality for Active Directory Federation Services (AD FS) to help system administrators provide secure access to an AD FS server. By using Web Application Proxy, system administrators can choose how end users should authenticate themselves to a web application and which users are authorized to use a web application.
	< Previous Next > Configure Cancel

10. Click Next. The Federation Server page appears.

Web Application Proxy Configure	ation Wizard	×
Federation Serve	n DESTINATION SERVER igwap.igaditfam.com	ł. n
Welcome Federation Server AD FS Proxy Certificate Confirmation Results	Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization. Federation service name:	
	Enter the credentials of a local administrator account on the federation servers. User name: administrator Password:	
	< Previous Next > Configure Cancel	

- **11.** 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.

Sa Web Application Proxy Configu	ration Wizard	×
AD FS Proxy Certificate		DESTINATION SERVER igwap.igadfsfarm.com
Welcome	Select a certificate to be used by the AD FS proxy:	
Federation Server	*.igadfsfarm.com	~ View
AD FS Proxy Certificate		
Results		
	2	
	-0	
	< Previous Next > Confi	gure Cancel

- **12.** Select the certificate for the AD FS proxy. The certificate should be the one with the Federation Service name as the subject.
- 13. Click Next. The Confirmation page appears.
- **14.** Review the settings on the Confirmation page. If required, you can copy the **PowerShell cmdlet** to automate additional installations.
- 15. Click Configure. The Results page appears.
- 16. In the **Results** page, verify that the configuration was successful and then click **Close**.

Publishing AD FS 4.0 sample application on WAP

To publish AD FS 4.0 sample application on WAP

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

💐 Remote Access Management Console			-	×
<		>	Tasks	
1 Configuration	PUBLISHED WEB APPLICATIONS	a .		
Web Application Proxy	All published web applications 0 total	General		^
Operations Status		Publish		
	No web applications are currently published. To publish a web application, click Publish.	Refresh		
igwap				

- 2. In the Navigation pane, click Web Application Proxy.
- 3. In the Tasks pane, click Publish. The Publish New Application Wizard appears.

Sa Publish New Application Wizard			×
Welcome		CONNECTED TO AD FS nlb.igadfsfarm.com	
Welcome Preauthentication	Welcome to the Publish New Application Wizard. This wizard helps you publish a new web application through Web Application Proxy.		
Supported Clients Relying Party			
Publishing Settings Confirmation	\searrow		
Results			
	< Previous Next > Publis	sh Cancel	

4. On the **Publish New Application Wizard Welcome** page, click **Next**. The Preauthentication page appears.

💐 Publish New Application Wizard		×	
Preauthentication	CONNECTED TO AD FS nib.igadfsfarm.com		
Welcome	Specify the preauthentication method:		
Preauthentication	 Active Directory Federation Services (AD FS) 		
Supported Clients	All unauthenticated client requests are redirected to the federation server. After successful		
Relying Party	authentication by AD FS, client requests are forwarded to the backend server. Web Application Proxy can also provide credentials to backend servers that are configured to use Integrated Windows		
Publishing Settings	authentication.		
Confirmation	O Pass-through		
Results	No preauthentication is performed by Web Application Proxy. All requests are forwarded to the backend server.		
	< Previous Next > Publish Cancel		

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.

Sa Publish New Application Wizard		×
Relying Party	CONNECTED TO AD F nlb.igadfsfarm.con	5
Welcome Preauthentication Supported Clients Relying Party Publishing Settings Confirmation Results	Select the AD FS relying party for this application: Filter P Name Image: Compared and the second and the	
	< Previous Next > Publish Cancel	

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.

Sublish New Application Wizard	d	>	×
Publishing Setting	gs con	NECTED TO AD FS Ilb.igadfsfarm.com	
Welcome Preauthentication Supported Clients Relying Party Publishing Settings Confirmation Results	Specify the publishing settings for this web application. Name: igwap This name will appear in the list of published web applications. External URL: https://nlb.igadfsfarm.com/claimapp/ External certificate: *.igadfsfarm.com v I Enable HTTP to HTTPS redirection Backend server URL: https://nlb.igadfsfarm.com/claimapp/	View	
	< Previous Next > Publish	Cancel	

- 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.
💱 Publish New Application Wizard	3	×
Confirmation	CONNECTED TO AD FS nbigadfsfarm.com	1
Welcome Preauthentication Supported Clients	The following PowerShell command will be run when you click Publish. It can also be used to set up additional published applications. If you want to re-use the command, copy it before you click Publish.	
Relying Party Publishing Settings	Add-WebApplicationProxyApplication -BackendServerU1 https://nlbigadfsfarm.com/claimapp/ -ExternalCertificateThumbprint '163AACF451F42DA5621A6052FF0748758C9A97DD'	
Confirmation Results	-EnableH11PRedirect:Strue -ExternalUrl 'https://nlb.igadfsfarm.com/claimapp/' -Name 'igwap' -ExternalPreAuthentication ADFS -ADFSRelyingPartyName 'nlb.igadfsfarm.com'	
	To publish the web application, click Publish.	
	< Previous Next > Publish Cancel	

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.

Publish New Application Wizard			
Results		CONNECTED TO AD FS adfs1.isapi.com	
Welcome Preauthentication RelyIng Party Publishing Settings Confirmation Results	Web application Entrust Demo - test app published successfully.		
	< Previous Next > Clos	e Cancel	

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 IdentityGuard Servers

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

- 1. Upon startup, the first Entrust IdentityGuard 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 IdentityGuard Server, then the solution fails over to the next available Entrust IdentityGuard 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 IdentityGuard Server. The default interval is one hour.

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

To configure failover for Entrust IdentityGuard 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 IdentityGuard 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 IdentityGuard 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 IdentityGuard 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 IdentityGuard Server being defined.

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

```
<ServerList>

<IdentityGuardServer>

<AuthenticationService

url="https://igserver1.mydomain.com:8443/IdentityGuardAuthService/servi

ces/AuthenticationServiceV11"/>

</IdentityGuardServer>

</ServerList>
```

This completes the definition of one Entrust IdentityGuard Server.

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

```
<ServerList>
     <IdentityGuardServer>
        <AuthenticationService
url="https://igserver1.mydomain.com:8443/IdentityGuardAuthService/servi
ces/AuthenticationServiceV11"/>
      </IdentityGuardServer>
      <IdentityGuardServer>
        <AuthenticationService
url="https://igserver2.mydomain.com:8443/IdentityGuardAuthService/servi
ces/AuthenticationServiceV11"/>
      </IdentityGuardServer>
      <IdentityGuardServer>
        <AuthenticationService
url="https://igserver3.mydomain.com:8443/IdentityGuardAuthService/servi
ces/AuthenticationServiceV11"/>
      </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 IdentityGuard Servers.

Appendix C: Known issues

There are no known issues.