

# **Entrust IdentityGuard**

**Desktop 12.0 for Microsoft® Windows®**

## **Administration Guide**

**Document issue: 4.0**

**Date of Issue: February 2020**

Copyright © 2020 Entrust Datacard. All rights reserved.

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.

This 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.

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.

## About this guide .....9

Revision information .....	10
Audience .....	11
Documentation conventions .....	12
Note and Attention text .....	12
Related documentation .....	14
Obtaining additional documentation .....	15
Documentation feedback .....	15
Obtaining technical assistance .....	16
Technical support .....	16
E-mail address .....	16
Professional Services .....	16
Training .....	17

## About Entrust IdentityGuard Desktop for Microsoft Windows .....19

Overview .....	20
Authentication overview .....	21
User experience .....	21
Deployment and management .....	24
Windows Login feature system components .....	25
Microsoft Windows client .....	25
Fingerprint scanner .....	25
Entrust IdentityGuard Server .....	26
Repository .....	26
Finding version information .....	27

**How Entrust IdentityGuard Desktop for Windows works .....29**

- Authentication with Entrust IdentityGuard Desktop for Windows ..... 30
  - Overview ..... 30
  - Offline challenges ..... 30
    - Offline grid challenges ..... 31
    - Offline token challenges ..... 31
- The user authentication process ..... 33
  - First-factor authentication ..... 34
  - Biometric authentication ..... 35
    - Grid authentication ..... 36
  - Token authentication ..... 38
  - OTP authentication ..... 41
  - Mobile soft token (TVS) authentication ..... 44
    - Passwordless authentication ..... 47
  - Online Question and Answer (Q&A) ..... 49
  - Offline Question and Answer (Q&A) ..... 51
  - Offline token ..... 54
    - How the offline token works ..... 57
    - Personal verification numbers ..... 58
    - Temporary PIN authentication ..... 59
- Biometric enrollment with the fingerprint enrollment client ..... 64
  - Accessing the biometric self-service module enrollment page ..... 64
- Users without Entrust IdentityGuard ..... 69

**Installing and configuring Entrust IdentityGuard Desktop for Microsoft Windows  
71**

- Preparing for installation ..... 72
  - Setting up users ..... 72
  - Gathering custom installation data ..... 73
  - Communication between Desktop for Microsoft Windows and the Entrust IdentityGuard Server ..... 73

Understanding Desktop for Microsoft Windows settings	75
Configuring the Entrust IdentityGuard Server settings	75
Configuring the Self-Service Module settings for password reset	75
Specifying other allowed Credential Providers	76
Including additional certificates	76
Disabling revocation checking	76
Configuring the group type	77
Configuring authentication options	77
Customizing temporary PIN instructions	78
Configuring offline authentication options	78
Specifying the maximum offline challenge attempts	79
Specifying the maximum number of Q&A attempts	79
Specifying the offline temporary PIN lock-out time	79
Customizing the logo on the login screen	80
About Microsoft Windows Installer	81
What is an administrative installation?	81
What is a transform file?	81
Windows Installer logging	82
Customizing the Entrust IdentityGuard Desktop for Microsoft Windows installation package	83
Using the custom installation wizard	84
Installing biometric drivers	106
Applying your custom transform file during installation	107
Testing the installation package	107
Providing the installation package as an executable or as a Windows Installer file	108
Distributing the installation package	109
Making the installation package available on the network	109
Making the installation package available on the Web	110
Using third-party software distribution tools	111
Performing a silent installation	111
Modifying silent installation options	112
Creating an administrative installation	113
Fresh installation: no existing Entrust IdentityGuard Desktop for Microsoft Windows software on users' computers	113
Assumptions	114

Administrative installation package contents .....	114
Adding a patch or service pack to an existing installation .....	115
Assumptions .....	116
Administrative install package contents .....	117
Saving the offline registry key when upgrading .....	119

## **Troubleshooting .....121**

Logging .....	122
Logging for the desktop client .....	122
Logging for the fingerprint enrollment client .....	122
Loss of Entrust credential provider after a reboot .....	124
Error messages .....	125

## **Customizing the installation package .....135**

Entrust IdentityGuard Server information worksheet .....	136
Configure group type worksheet .....	137
Configure options for Windows Login .....	138
Configure options for offline Windows Login .....	139
Entrust IdentityGuard Self-Service Module information worksheet .....	140
Include additional certification providers worksheet .....	141
Adding certification providers from a file .....	142
Include additional certificates worksheet .....	143
Include additional registry values worksheet .....	144

## **Registry settings .....145**

Registry settings under 'Domains' .....	146
Registry settings under 'WIGL' .....	147
Registry settings under 'DomainsAlias' .....	155
Registry settings under 'AllowCPs' .....	156
Registry settings under 'SSM' .....	157
Registry settings under 'SSMDomains' .....	159
Registry settings under 'Credential Providers' .....	160

## **IdentityGuard Desktop client integration with SSM .....161**

Desktop client and SSM integration overview .....	162
---	-----

Enabling Active Directory password reset . . . . .	163
Enabling other self-administration operations, in addition to password reset . . . . .	164
Do users need to log in to the Self-Administration Actions page? . . . . .	164
How do users access the password reset pages? . . . . .	164
Enabling a link to the Actions page, and customizing the links on this page . . . . .	164
List of default URLs that are accessible by clicking the self-service link on the Windows login screen . . . . .	165
Examples . . . . .	166





## About this guide

This guide provides detailed information for administrators to plan, deploy, administer, and troubleshoot the Entrust IdentityGuard Desktop client for Microsoft Windows. This chapter includes the following topics:

- [“Revision information” on page 10](#)
- [“Audience” on page 11](#)
- [“Documentation conventions” on page 12](#)
- [“Related documentation” on page 14](#)
- [“Obtaining additional documentation” on page 15](#)
- [“Obtaining technical assistance” on page 16](#)

# Revision information

**Table 1:** Revisions in this document

Document issue and date	Section	Description
4.0 February 2020	"Registry settings"	<ul style="list-style-type: none"><li>Added missing registry setting, <a href="#">"AuthenticateLocalUsers"</a> on page 147</li></ul>
3.0 February 2020	"Registry settings"	<ul style="list-style-type: none"><li>Added <code>EnableUPNUserName</code> registry setting to the section <a href="#">"Registry settings under 'WIGL'"</a> on page 147.</li><li>Add a new section, <a href="#">"Registry settings under 'DomainsAlias'"</a> on page 155</li></ul>
2.0 May 2019	"Registry settings"	Added <code>EIGLoggerFileSizeForRollOn</code> and <code>EIGLoggermaxBackupIndex</code> registry settings to the section <a href="#">"Registry settings under 'WIGL'"</a> on page 147.
1.0 January 2019	All sections	This is the first issue of this guide.

# Audience

The intended audience of this document is administrators deploying and administering the Windows Login feature of Entrust IdentityGuard Desktop for Microsoft Windows.

To use the Windows Login feature information in this guide, you should have a basic understanding of the following:

- Entrust IdentityGuard Server
- Secure Sockets Layer (SSL) protocol
- Microsoft® Windows® client and server operating systems
- Microsoft® Windows® Installer

# Documentation conventions

The following table describes documentation conventions that appear in this guide:

**Table 2:** Typographic conventions

Convention	Purpose	Example
<b>Bold</b> text (other than headings)	Indicates graphical user interface elements and wizards	Click <b>Next</b> .
<i>Italicized</i> text	Used for book or document titles	<i>Entrust TruePass 7.0 Deployment Guide</i>
<a href="#">Blue</a> text	Used for hyperlinks to other sections in the document	Entrust TruePass supports the use of many types of <a href="#">digital ID</a> .
<u><a href="#">Underlined blue</a></u> text	Used for Web links	For more information, visit our Web site at <a href="http://www.entrustdatacard.com">www.entrustdatacard.com</a> .
Courier type <code>[courier type]</code>	Indicates installation paths, file names, Windows registry keys, commands, and text you must enter	Use the <code>entrust-configuration.xml</code> file to change certain options for Verification Server.
Angle brackets < >	Indicates variables (text you must replace with your organization's correct values)	By default, the <code>entrust.ini</code> file is located in <code>&lt;install_path&gt;/conf/security/entrust.ini</code> .
Square brackets <code>[courier type]</code>	Indicates optional parameters	<code>dsa passwd [-ldap]</code>

## Note and Attention text

Throughout this guide, there are paragraphs set off by ruled lines above and below the text. These paragraphs provide key information with two levels of importance, as shown below.



### **Note:**

Information to help you maximize the benefits of your Entrust product.

**Attention:**

Issues that, if ignored, may seriously affect performance, security, or the operation of your Entrust product.

---

## Related documentation

This section provides a list of useful reference material. Some of these documents are also mentioned throughout this guide in relevant places as related reading material.

The *Entrust IdentityGuard Administration Guide* contains information required by the Entrust IdentityGuard administrator.

# Obtaining additional documentation

Entrust Datacard product documentation, white papers, technical notes, and a comprehensive Knowledge Base are available through Entrust Datacard TrustedCare Online. If you are registered for our support programs, you can use our Web-based Entrust Datacard TrustedCare Online support services at:

<https://trustedcare.entrustdatacard.com/>

## Documentation feedback

You can rate and provide feedback about product documentation by completing the online feedback form. Any information that you provide goes directly to the documentation team and is used to improve and correct the information in our guides. You can access this form by:

- clicking the *Report any errors or omissions* link located in the footer of PDF documents (see bottom of this page).
- following this URL: <http://go.entrust.com/documentation-feedback>.

# Obtaining technical assistance

Entrust Datacard recognizes the importance of providing quick and easy access to our support resources. The following subsections provide details about the technical support and professional services available to you.

## Technical support

Entrust Datacard offers a variety of technical support programs to help you keep Entrust products up and running. To learn more about the full range of technical support services, visit our Web site at:

<https://www.entrust.com/get-support/enterprise-support/>

If you are registered for our support programs, you can use our Web-based support services.

Entrust Datacard TrustedCare Online offers technical resources including product documentation, white papers and technical notes, and a comprehensive Knowledge Base at:

<https://trustedcare.entrustdatacard.com/>

If you contact Customer Support, please provide as much of the following information as possible:

- your contact information
- product name, version, and operating system information
- your deployment scenario
- description of the problem
- copy of log files containing error messages
- description of conditions under which the error occurred
- description of troubleshooting activities you have already performed

## E-mail address

The e-mail address for Customer Support is:

[support@entrust.com](mailto:support@entrust.com)

## Professional Services

The Entrust Datacard team assists organizations around the world to deploy and maintain secure transactions and communications with their partners, customers, suppliers and employees. Entrust Datacard offers a full range of professional services to deploy our solutions successfully for wired and wireless networks, including



planning and design, installation, system integration, deployment support, and custom software development.

Whether you choose to operate your Entrust Datacard solution in-house or subscribe to hosted services, Professional Services will design and implement the right solution for your organization's needs. For more information about Professional Services please visit our Web site at:

<https://www.entrust.com/services>

## Training

Through a variety of hands-on courses, Entrust Datacard delivers effective training for deploying, operating, administering, extending, customizing and supporting any variety of Entrust Datacard digital identity and information security solutions.

Delivered by training professionals, Entrust Datacard's professional training services help to equip you with the knowledge you need to speed the deployment of your security platforms and solutions. Please visit our training website at:

<http://www.entrust.com/training>



# About Entrust IdentityGuard Desktop for Microsoft Windows

This chapter includes the following general information about the Windows Login feature of Entrust IdentityGuard Desktop for Microsoft Windows.

- [“Overview” on page 20](#)
- [“Windows Login feature system components” on page 25](#)
- [“Finding version information” on page 27](#)

# Overview

Entrust IdentityGuard Desktop for Microsoft Windows is a small-footprint client that communicates with the Entrust IdentityGuard Server. The Entrust IdentityGuard Server is a server-based software product that authenticates and manages users and their authentication data.

Entrust IdentityGuard Desktop for Microsoft Windows provides strong second-factor authentication to Windows Desktop Login (online or offline). Before users are allowed to log in to a protected domain from their computers, they are required to pass second-factor authentication. Local users of the computer on which the Entrust IdentityGuard Desktop for Microsoft Windows is installed are not required to use second-factor authentication to log in.

Entrust IdentityGuard Desktop for Microsoft Windows contains a credential provider. The credential provider responds to these use cases:

- workstation login
- workstation unlock
- password change
- credential prompt (run elevated)

When you install the Entrust IdentityGuard Desktop for Microsoft Windows package, the installation installs a Credential Provider Filter. You can opt to have this filter replace default Windows behavior, or you can have more than one credential provider coexist with this filter to handle different use cases. This guide provides information about installing and using the Windows Login feature of Entrust IdentityGuard Desktop for Microsoft Windows.

## Authentication overview

Entrust IdentityGuard Desktop for Microsoft Windows supports:

- Password-less authentication, which does not require a user to submit a password for authentication after the initial log in. A user performs only Entrust IdentityGuard-based second factor authentication.
- Grid authentication, based on an assortment of characters in row and column format allowing the user to respond to a log on challenge with characters drawn from co-ordinates in the grid.
- Token authentication, using tokens from Entrust or another vendor. Entrust IdentityGuard supports both response-only and challenge-response tokens.
- Personal verification number (PVN), which can provide additional security when used in addition to their grid or token response.
- Temporary personal identification number (PIN) which can be assigned by the administrator to provide access for first-time authentication, or if a user loses their grid or token.
- Knowledge-based question and answer (Q&A) for online and offline use, which can be set up on the Entrust IdentityGuard Server using Entrust IdentityGuard Self-Service Server (also called Entrust IdentityGuard Self-Service Module).
- Mobile soft token authentication (TVS), an out-of-band authentication challenge is sent to the user's mobile device.
- Biometric authentication (fingerprint), using fingerprint data captured using the biometric enrollment client that can be installed at the same time as the desktop client
- OTP authentication, an out-of-band one-time password (OTP) is sent to a user's contact information (email address or phone number).
- Combined multifactor authentication login, which evaluates first- and second-factor authentication challenges at the same time. This method complies with the Payment Card Industry Data Security Standards.
  - Combined multifactor authentication supports Grid, Token and Mobile Soft Token Authentication.

## User experience

When Entrust IdentityGuard Desktop for Microsoft Windows is installed, users are required to respond to a second-factor authentication challenge when they log in to a protected domain or perform certain tasks. The form of second-factor authentication challenge used depends on what has been configured for users in the Entrust IdentityGuard Server. The list that follows describes how Entrust IdentityGuard Desktop for Microsoft Windows behaves in various scenarios:

### Windows login

- The user is challenged for a Windows user name and password.
- After the user responds correctly, a second-factor authentication challenge is displayed for the user.
- If the user enters the correct response, they are granted access to the computer.

### Fallback authentication

- If biometric authentication is not successful, users have the option to retry biometric authentication or authenticate using either a grid, token, or mobile ST (TVS) as configured in Entrust IdentityGuard policy.

### Mobile soft token (TVS) authentication

- An out-of-band authentication challenge is sent to the user's mobile device. The user selects **Confirm** to access the protected resource.
- If the authentication request was not initiated by the user or appears fraudulent, the user can select **Cancel** to deny access to the resource, or select **Concern**, in which case the authentication request is canceled.

### OTP authentication

- An out-of-band one-time-password authentication challenge is sent to the user's contact information (email address or phone number). The user enters the OTP for second factor authentication.

### Missing second-factor authenticator

- If the user does not have a grid or token (for example, if it is lost), they can enter a temporary PIN that the Entrust IdentityGuard Desktop for Microsoft Windows will validate. The temporary PIN option is not available if you use biometric authentication.

### Combined multifactor authentication

- Combined Multifactor Authentication is similar to Windows login in case of valid authentication scenario.
- Combined multi-factor authentication login evaluates first- and second-factor authentication challenges at the same time.
  - In the event of invalid authentication, it behaves as follows:
  - The user is challenged for a Windows user name and password.
  - If the user enters an invalid response, a second-factor authentication challenge is displayed to the user.

- If the user enters the correct response, the user is shown error message saying one or more of you responses is in-correct.

**Note:**

If you do not want to offer users the option to log in with a temporary PIN, you can hide this link. For more information, see [EnableOnlineTempPINAuth](#) in ["Registry settings under 'WIGL'" on page 147](#).

**Lockout due to incorrect responses**

- If the user enters multiple incorrect responses, exceeding the lockout limit, they are locked out of the computer.

**Offline authentication**

- If the user is offline, they can use their grid or token (OTP) (and PVN, if applicable) if they were required by Entrust IdentityGuard policy the last time the user was online. Windows Login will validate the response against hash values from the challenge responses of the previous successful authentication. These hash values are stored in the Windows registry.
- If the user is offline, they can enter an offline temporary PIN that the Windows Login feature will validate against the value of the offline temporary PIN stored (in encrypted format) in its repository.
- If the user is offline, they will still be able to use their PVN, if the PVN was required by Entrust IdentityGuard during the previous online session.
- If the user is offline and Offline Question and Answer (Q&A) has been configured, they will be able to use the responses stored on their computer to log in.
- If the user is offline and Offline Question and Answer (Q&A) has been configured, they will be able to use the responses stored on their computer to log in.
- If the user is offline and Offline Token has been configured, the user can use a one-time-password (OTP) to log in.
- If the user is offline and Offline Token has been configured to require a PVN, the user can use the PVN to log in.
- If the user is offline, they cannot use biometric (fingerprint) authentication. If Offline Question and Answer (Q&A) has been configured, they will be able to use the responses stored on their computer to log in.

## Deployment and management

To make deployment and management easy, Entrust IdentityGuard Desktop for Microsoft Windows uses Microsoft Windows Installer technology, allowing:

- faster and easier installation
- the ability to repair installations
- powerful installation rollback capabilities that restore the desktop to the condition it was in prior to an unsuccessful installation
- the ability for users to install the Entrust IdentityGuard Desktop for Microsoft Windows software from a specified URL using a Web browser

Administrators use the **Custom Installation** wizard that comes with Entrust IdentityGuard Desktop for Microsoft Windows to configure the applications before deployment. If administrators want to modify any of these settings after deploying the application, they can

- use existing Microsoft tools to modify the Microsoft registry on the user's desktop.
- create a new installation package to distribute to users by running the **Entrust IdentityGuard Desktop Custom Installation** wizard again.

See [“Installing and configuring Entrust IdentityGuard Desktop for Microsoft Windows” on page 71](#) for further customization and installation information.

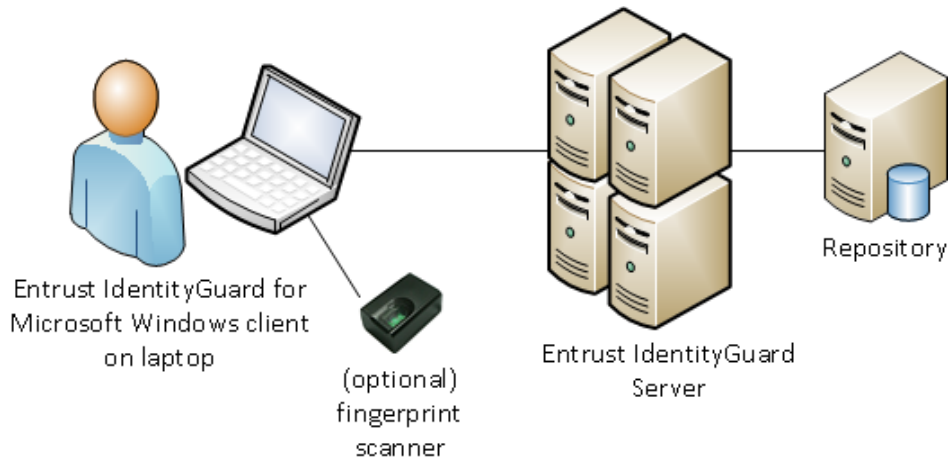


# Windows Login feature system components

This section describes the system components for the Windows Login feature.

[Figure 1 on page 25](#) illustrates the Windows Login basic system components.

**Figure 1:** Windows Login system components



## Microsoft Windows client

Entrust IdentityGuard Desktop for Microsoft Windows is a small-footprint client that communicates with Entrust IdentityGuard Server. The Windows Login feature forces users to use second-factor authentication when they log in to their Microsoft Windows desktop computer using a user ID with Entrust IdentityGuard protection.

## Fingerprint scanner

The fingerprint scanner is an optional hardware component that is required to enroll biometric data (fingerprints) if biometric authentication is used. The fingerprint scanner interacts with the fingerprint enrollment client, an application that can be installed using the same wizard that installs the Entrust IdentityGuard Desktop client. The fingerprint enrollment client uses drivers that are installed as part of the enrollment client installation.

# Entrust IdentityGuard Server

---

**Note:**

Entrust IdentityGuard Server version 12.0 patch 25610 (or later) is required for this integration with Entrust IdentityGuard Desktop. To check that you are using the correct version, open the Entrust IdentityGuard Administration interface and ensure that the software version number at the bottom of the page is 12.0 patch 25610 or later.

---

Entrust IdentityGuard is a server-based software product installed in an organization's current infrastructure. It is the main component of the Entrust IdentityGuard system. It includes the applications and interfaces required to authenticate and manage users and their authentication data. Entrust IdentityGuard Server uses a repository to store user data.

## Repository

Entrust IdentityGuard uses your existing repository to store user data. When you generate grid, token, or other authentication data for the user, Entrust IdentityGuard writes the sensitive data in encrypted form to the repository. The data is retrieved from the repository during user authentication.

Entrust IdentityGuard stores user data in an existing LDAP-compliant directory (Microsoft Active Directory, for example) or a database.

# Finding version information

Use the following procedure to display the version of your installation.

## To locate the version of the Entrust IdentityGuard Desktop for Microsoft Windows software

- 1 Open the Windows **Control Panel** and access **Programs and Features**.
- 2 The Entrust IdentityGuard Desktop for Windows version appears in the **Version** column.

The exact version number, including the build number, is displayed on the files Details tab for individual DLL files. The DLL files are located in:

- C:\Windows\System64\eigcp64.dll
- C:\Windows\System64\eigcpfilter64.dll
- C:\Program Files\Entrust\IdentityGuard Desktop\1033\eigcpenu64.dll
- C:\Program Files\Entrust\IdentityGuard Desktop\1033\eigcpevenu64.dll



### **Note:**

Files for the 32-bit version have 32 rather than 64 in the file name.

---



# How Entrust IdentityGuard Desktop for Windows works

This chapter describes user interaction with Entrust IdentityGuard Desktop for Windows for authentication and biometric fingerprint enrollment:

- [“Authentication with Entrust IdentityGuard Desktop for Windows” on page 30](#)
- [“Biometric enrollment with the fingerprint enrollment client” on page 64](#)
- [“Users without Entrust IdentityGuard” on page 69](#)

# Authentication with Entrust IdentityGuard Desktop for Windows

Your organization may use one or more second-factor methods for authenticating users with the Windows Login feature. The following topics are discussed in this section:

- [“Overview” on page 30](#)
- [“Offline challenges” on page 30](#)
- [“The user authentication process” on page 33](#)

## Overview

After entering their Windows user name and password, the Entrust IdentityGuard user sees a second dialog, which prompts them with a challenge.

To get access to the desktop and network, the user enters the grid or token response to the challenge, a temporary PIN, or uses an attached fingerprint scanner to read their fingerprint and compare it with the one enrolled with Entrust IdentityGuard.

If the user’s response is correct, the user is able to access their desktop. Whether the desktop is accessible to users without Entrust IdentityGuard authentication set up is configurable when the Entrust IdentityGuard installation package is created. See [“To create a custom installation package” on page 84](#) for more information about configuring the authentication options.

The server keeps track of the number of attempts, and locks the user out after the maximum number of incorrect attempts is reached. The number of allowable attempts for an online Windows login is configured using the Entrust IdentityGuard Server. See the *Entrust IdentityGuard Administration Guide* for further information.

If a user is online and clicks **Use Temporary PIN**, Entrust IdentityGuard displays a screen that allows the user to enter a temporary PIN. The user can click a link to open a help message that describes how to get a temporary PIN if they do not have one. See [“To create a custom installation package” on page 84](#) for more information about customizing this message.

## Offline challenges

Entrust IdentityGuard Desktop for Windows can use strong second-factor authentication to log in users, even if they are temporarily out of contact with the Entrust IdentityGuard Server. To do this, Desktop for Windows stores challenges from online sessions. In the case of a new install with an offline login, there are no stored challenges, so no offline challenges are possible.

The following types of challenges can be used offline:

- "Offline grid challenges"
- "Offline token challenges"

## Offline grid challenges

---



### Attention:

Offline grid responses must be entered exactly as they were when the user responded to the challenge online. For example, if the user successfully entered Ao1 instead of A01 (the Entrust IdentityGuard Server accepts fuzzy responses) the user must also use Ao1 to log in offline. A01 will not be accepted. Offline responses are also case sensitive.

---

- offline Q&A (question and answer)
  - offline temporary PIN
- 



### Note:

The policy configured on the Entrust IdentityGuard Server must allow enough space for the stored shared secrets.

In the **Shared Secret Policy Category**, set the size of the **Total Maximum Size in Kilobytes** to take into account that each user's computer has an offline temporary PIN that takes up approximately 100 bytes of shared secret storage. Set the **Maximum Number of Shared Secrets** to the number of computers that each user might be expected to use.

The defaults (4 KB of space and 10 secrets) should be sufficient unless there are other applications using shared secrets. If either field is set to 0 then offline authentication using an offline temporary PIN will not work.

---

## Offline token challenges

The Entrust IdentityGuard Desktop for Windows client supports offline token download.

If offline token has been configured, the login window includes a checkbox to download offline tokens. By default, the checkbox is not selected.

While online, the user selects to download offline tokens to their PC. The download tokens are valid for a period of time based on the policy settings in Entrust

IdentityGuard server and the Windows registry setting for offline token login (see [“Registry settings under ‘WIGL’” on page 147](#)). If the PC remains offline for too long, the user will be unable to log into their PC until they complete a successful online login and download new token data.

If PVN is configured, then the user is also prompted to provide a PVN.

If the validation is successful, then the user is allowed to log in. An error message appears if the validation fails.



**Note:**

The policy configured on the Entrust IdentityGuard Server must allow for offline token challenge with or without PVN.

In the **Minor hours** setting, set the amount of time, in hours, that Entrust IdentityGuard Server will allow offline validation by OTP. In the **Max hours** setting, set the maximum amount of time, in hours, that Entrust IdentityGuard Server will allow offline validation by OTP.

Set the **Protection Level** to determine the level of cryptographic protection applied to the offline OTP data stored on the PC. The options are NORMAL, STRONG and VERY\_STRONG.

---



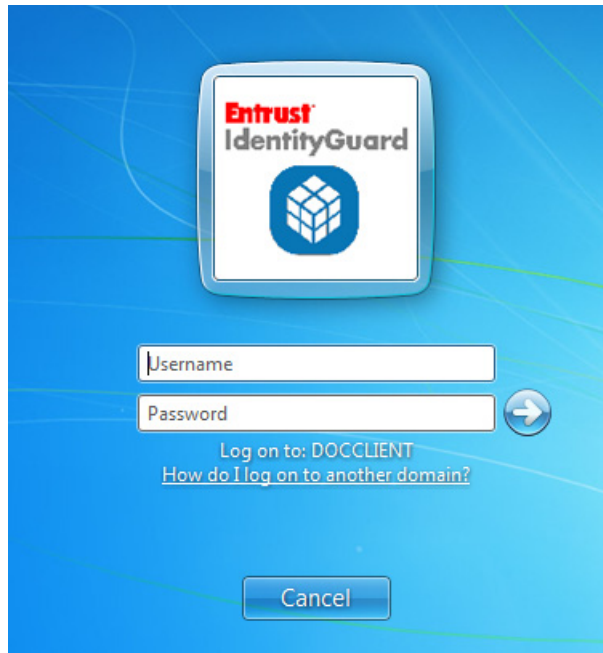
# The user authentication process

To log in to the network, Entrust IdentityGuard Desktop for Windows users must complete first and second-factor authentication challenges. These are determined by the user's configuration in Entrust IdentityGuard. The following authentication methods are discussed in this section.

- ["First-factor authentication" on page 34](#)
- ["Biometric authentication" on page 35](#)
- ["Grid authentication" on page 36](#)
- ["Token authentication" on page 38](#)
- ["OTP authentication" on page 41](#)
- ["Mobile soft token \(TVS\) authentication" on page 44](#)
- ["Online Question and Answer \(Q&A\)" on page 49](#)
- ["Online Question and Answer \(Q&A\)" on page 49](#)
- ["Personal verification numbers" on page 58](#)
- ["Temporary PIN authentication" on page 59](#)
- ["Passwordless authentication" on page 47](#)

## First-factor authentication

- 1 Upon first log in, default log in screen displays the Entrust IdentityGuard logo and fields for the user's user name and password.



Entrust IdentityGuard Desktop for Windows users begin logging into the domain by entering their user name and their Windows password. Entrust IdentityGuard Windows users must have a valid Windows userid in the protected domain. Users logging into the domain must be registered as a user in the Entrust IdentityGuard Server protecting the domain. Unregistered users may be treated differently (see [“Users without Entrust IdentityGuard” on page 69](#)).

- 2 Clicking the arrow icon brings the user to the second-factor authentication screen. The type of second-factor authentication depends on the user's configuration in Entrust IdentityGuard.



### Note:

After the user clicks the arrow button and the second-factor authentication screen appears, they cannot return to the first-factor login screen. If the user decides to back-out of second-factor authentication without completing the challenge, they must use the **Switch User** button.

## Biometric authentication

Biometric authentication with Entrust IdentityGuard is supported using the Entrust IdentityGuard Desktop for Microsoft Windows client application. Use of this authentication method requires configuration in the Entrust IdentityGuard Server and Entrust IdentityGuard Self-Service Module. For configuration information, see the *Entrust IdentityGuard Administration Guide* and the *Entrust IdentityGuard Self-Service Module Installation and Configuration Guide*.

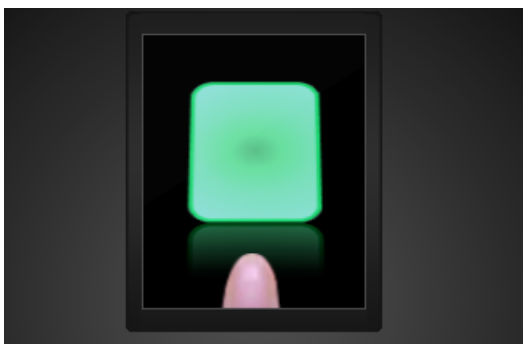
The fingerprint biometrics required for biometric authentication are captured using a fingerprint enrollment client that is available as part of the Entrust IdentityGuard Desktop for Microsoft Windows package (installed using the same installer).

As part of the fingerprint enrollment, users login to self-service website where they click the self-administration action link I'd like to enroll for fingerprint biometric authentication. For more information, see ["Biometric enrollment with the fingerprint enrollment client" on page 64](#).

Users of biometric authentication require a fingerprint scanner both to enroll their fingerprint data and to authenticate.

Biometric authentication to a Windows computer works as follows:

- 1 The user completes first-factor authentication successfully.
- 2 Entrust IdentityGuard presents the user with a biometric authentication challenge.



- 3 The user places one of the enrolled fingers on the fingerprint scanner attached to their Windows computer and holds it there until a green border appears around the fingerprint image on-screen.
- 4 Entrust IdentityGuard compares the scanned fingerprint with the biometric in its database and, if it matches, authenticates the user.
- 5 If the scanned fingerprint fails validation with Entrust IdentityGuard, the user is given the options to try again or to authenticate using a grid or token. After a configured number of failed authentication attempts, the user is locked out.

Biometric authentication is not supported in offline or remote login scenarios. For offline authentication, users can configure a question and answer challenge.

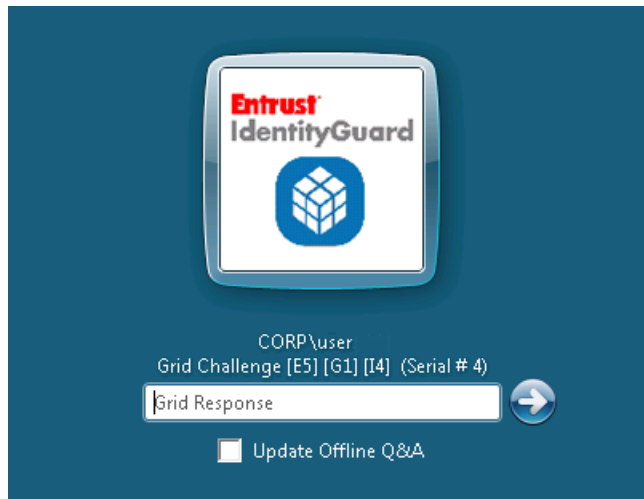
You can customize the biometric enrollment client with your logo. For more information, see `BiometricCustomLogoPath` in ["Registry settings under 'WIGL'" on page 147](#).

## Grid authentication

Users with grid authentication should be provided with an Entrust IdentityGuard grid before logging in. The grid contains an assortment of characters in a row and column format. You can require that your users also use a personal verification number (PVN), with the grid. See ["Personal verification numbers" on page 58](#).

Authentication works as follows:

- 1 The user completes first-factor authentication successfully.
- 2 Entrust IdentityGuard presents the user with a challenge based on their grid.



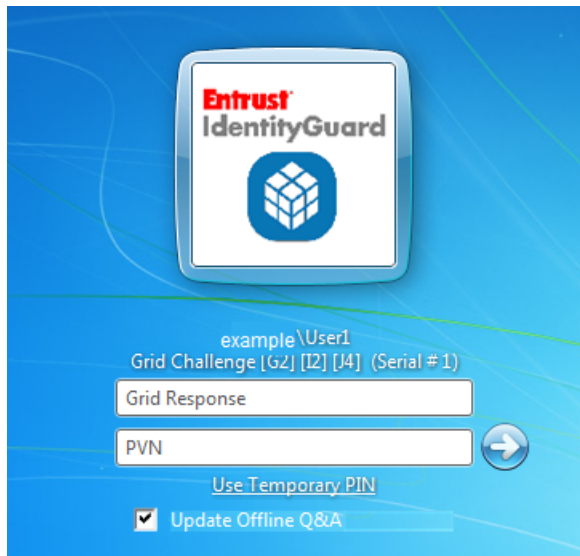
- 3 The user enters the values from their grid that correspond to the requested cell locations in the challenge. For example, the challenge shown above asks the user

to enter the characters in coordinates B2, F5, and I2. Using the grid shown in the graphic the correct response is 1, 9, and 7.

	A	B	C	D	E	F	G	H	I	J
1	1	1	J	0	D	2	K	1	1	F
2	H	1	2	V	P	Y	1	N	7	V
3	T	6	2	R	4	2	K	W	2	2
4	F	T	F	N	H	0	1	N	9	3
5	P	X	J	Y	6	9	K	8	5	9

By entering the correct response, users demonstrate that they possess the grid, thus providing second-factor authentication. Entrust IdentityGuard validates the entered values and authenticates the user.

- 4 If you have required your users to log in using both a grid card and a personal verification number (PVN), the login screen will also have a field for them to enter the PVN.



The image shows the Entrust IdentityGuard login interface. At the top is the Entrust IdentityGuard logo. Below it, the text "example \User1" and "Grid Challenge [G2] [I2] [J4] (Serial # 1)" are displayed. There are two input fields: "Grid Response" and "PVN". A blue arrow button is to the right of the PVN field. Below the input fields is a link "Use Temporary PIN" and a checkbox labeled "Update Offline Q&A" which is checked.

## Token authentication

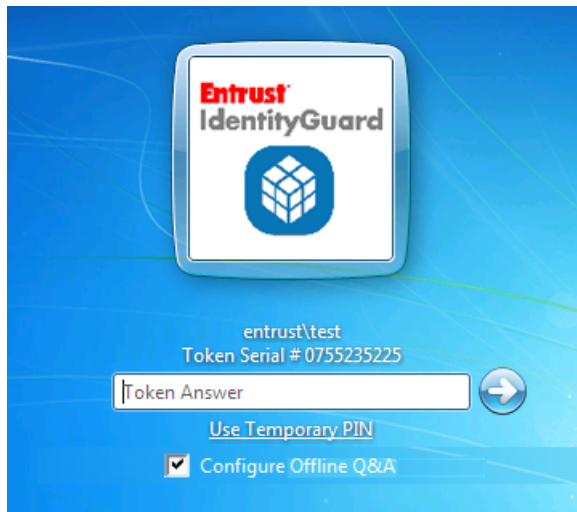
For token authentication, you provide each user with an token. A token is a small device that generates passwords. There are two types of tokens; response-only tokens and challenge-response tokens. You can require your users to use a personal verification number (PVN) with the token for additional security. See [“Personal verification numbers” on page 58](#).

Authentication works a little differently for the two token types.

### Response-only tokens

For response-only tokens, authentication works as follows:

- 1 The user completes first-factor authentication successfully.
- 2 Entrust IdentityGuard presents the user with a challenge based on the serial number of their token.



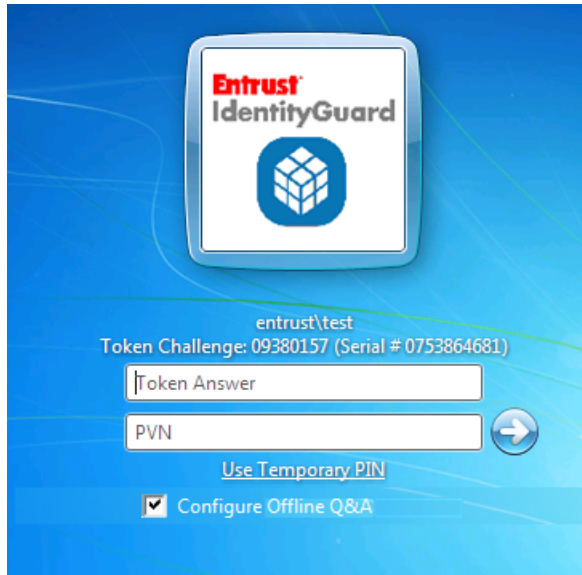
- 3 The user presses the button on their token to generate a password,



- 4 The user enters the password response.

By entering the correct response, users demonstrate that they possess the token thus providing a second-factor of authentication. Entrust IdentityGuard validates the values and authenticates the user.

- 5 If you have required your users to log in using both a token and a personal verification number (PVN), the login screen will also have a field for them to enter the PVN.

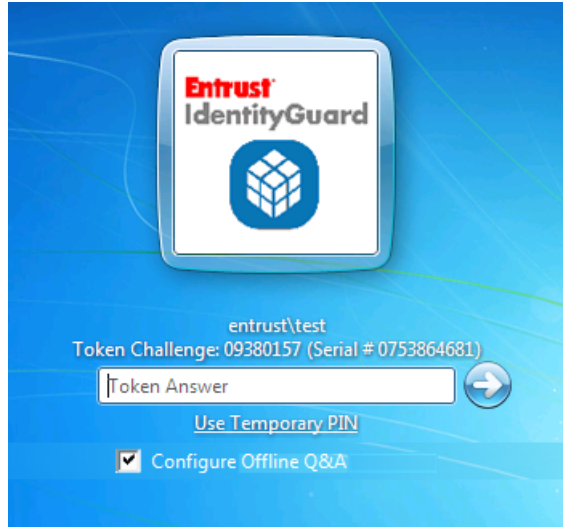


### Challenge-response tokens

For challenge-response tokens, authentication works as follows:

- 1 The user completes first-factor authentication successfully.

- 2 Entrust IdentityGuard presents a challenge code based on the serial number of their token.



- 3 The user enters the challenge into their token.
- 4 The user presses the button on their token to generate a dynamic password.
- 5 The user enters the dynamic password response.

By entering the correct response, users demonstrate that they possess the token, thus providing a second-factor of authentication. Entrust IdentityGuard validates the entered values and authenticates the user.
- 6 If you have required your users to log in using both a token and a personal verification number (PVN), the login screen will also have a field for them to enter the PVN.



## OTP authentication

With out-of-band one-time password (OTP) authentication, a user is sent an OTP to the user's contact information (email address or phone number).

OTP authentication can be delivered automatically or manually by requesting an OTP from the Entrust IdentityGuard administrator.

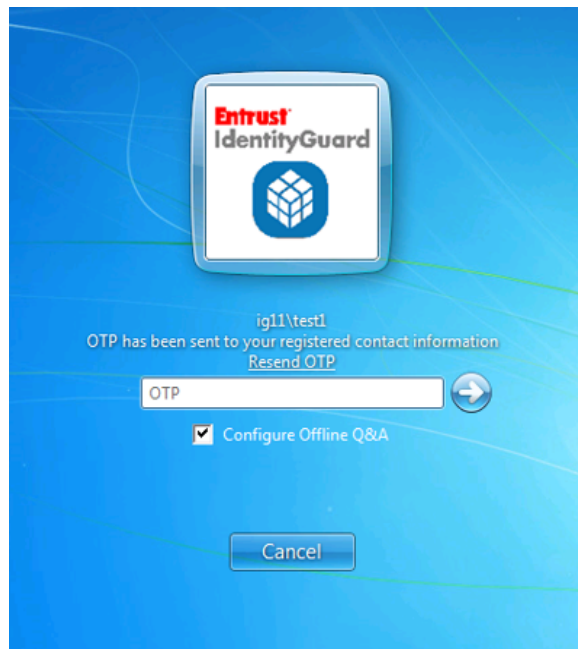
If the user's contact information, email address or phone number is enabled as the default delivery mechanism, then OTP will be delivered only to that delivery mechanism.

If a default delivery mechanism is not enabled for the user's contact information, then OTP will be delivered to all of the user's delivery mechanisms or the user's contact information.

### OTP automatic authentication

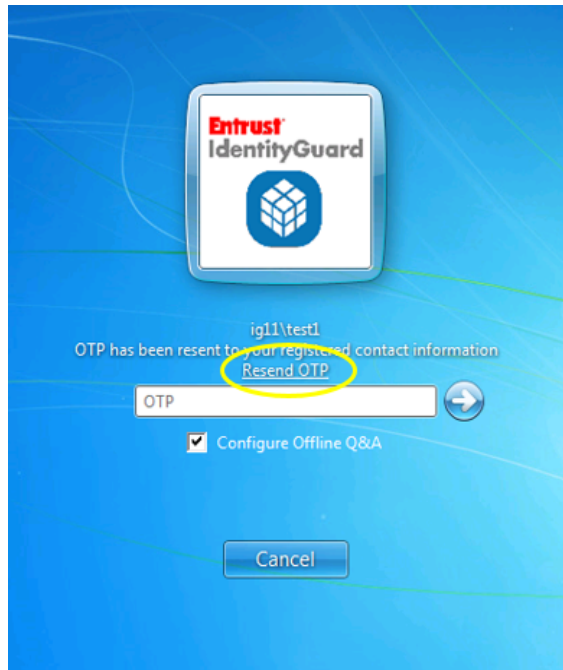
OTP automatic authentication works as follows:

- 1 The user completes first-factor authentication successfully.
- 2 Entrust IdentityGuard presents the user with a challenge based on their OTP.



- 3 The user enters their OTP that was delivered to their contact information (email address or phone number).

- 4 If required, the user can request a new OTP by clicking the Resend OTP link.



### OTP manual authentication

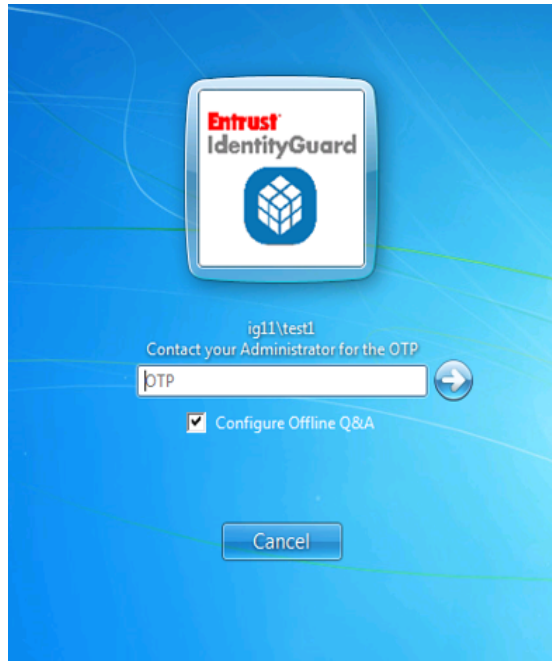
When OTP manual authentication is enabled, the user sends a request to the administrator for an OTP. The administrator sends the OTP to the user's contact information.

OTP manual authentication is enabled through the `EnableManualOTP` registry setting. See ["EnableManualOTP" on page 149](#) for more information.

OTP manual authentication works as follows:

- 1 The user completes first-factor authentication successfully.

- 2 Entrust IdentityGuard presents the user with a challenge based on their OTP.



- 3 The user contacts the Entrust IdentityGuard Administrator for a new OTP.
- 4 The Administrator shares the OTP with the user.
- 5 The user authenticates with the OTP provided by the Administrator.

## Mobile soft token (TVS) authentication

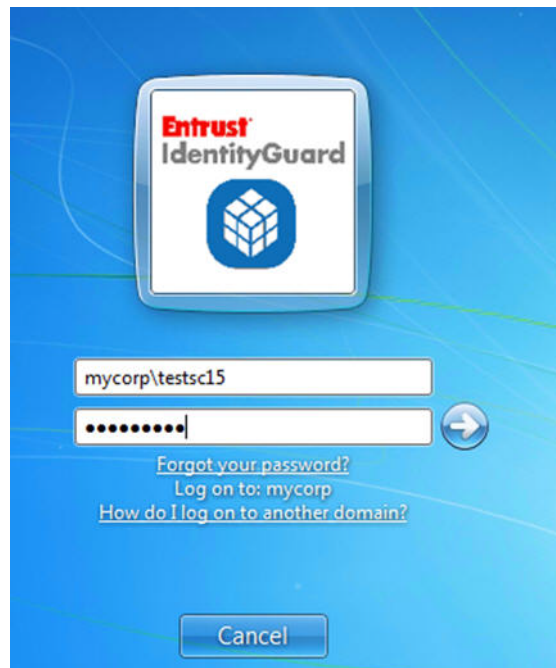
The Entrust IdentityGuard Mobile Soft Token app (formerly called the Entrust IdentityGuard Mobile OTP app) generates numbers that you use to authenticate to a Web site or to confirm transactions.

If you are connected to a cellular provider data network or Wi-Fi, you select the **Confirm** button to complete the action. If you are not, you enter the number shown in the app on the Web page to authenticate or to complete a transaction.

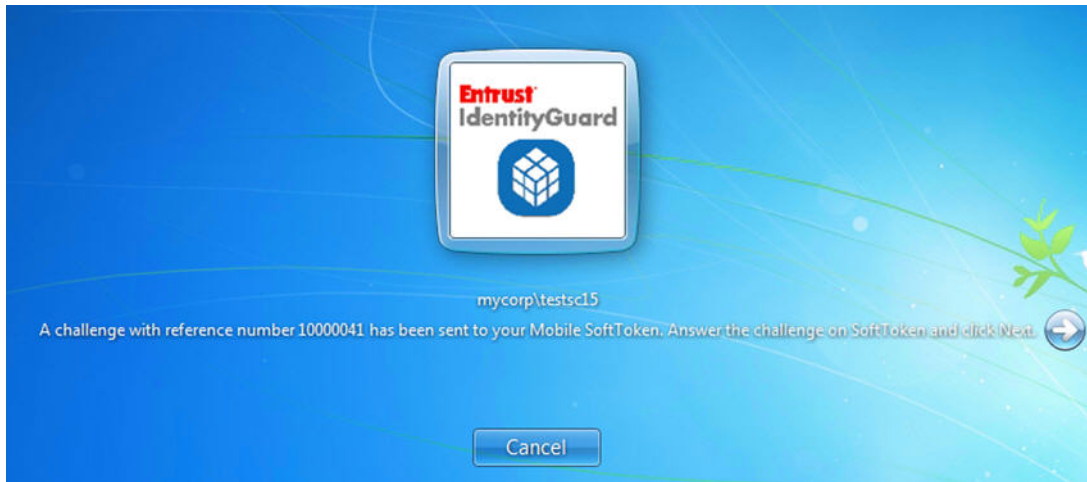
### Soft token authentication

Soft token authentication works as follows:

- 1 The user completes first-factor authentication successfully.



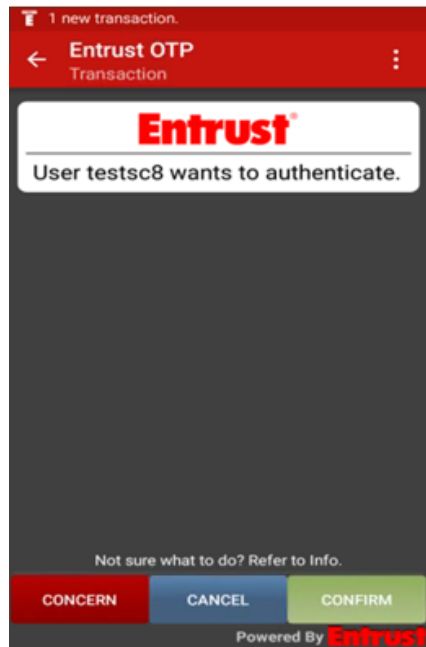
- 2 Entrust IdentityGuard presents the user with a challenge reference number that has been sent to their mobile soft token.



- 3 Open the Entrust Mobile Soft Token app on your mobile device and enter your PIN number.
- 4 On the Security Code or Identities screen, open the menu and select **New Transactions**.



5 The transaction details appear.



6 Select the appropriate response:

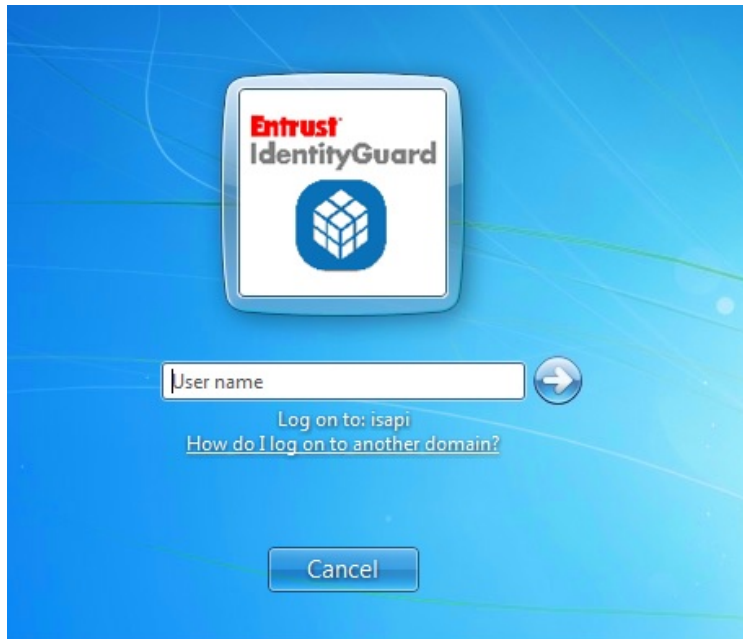
- If the information is correct, select **Confirm**.
- If you no longer want to proceed with the transaction, select **Cancel**.
- If the information is suspicious, select **Concern**.

If you are connected to a data network and online transactions are enabled, the action you chose is sent to your Identity Provider's Web site, for example, your banking Web site.

If online transactions are not enabled, enter the confirmation code shown in the app into your Identity Provider's Web site.

## Passwordless authentication

- 1 The default log in screen displays the Entrust IdentityGuard logo and fields for the user's user name and password.



- Entrust IdentityGuard Desktop for Windows users begin logging into the domain by entering their user name and their Windows password. Entrust IdentityGuard Windows users must have a valid Windows userid in the protected domain. Users logging into the domain must be registered as a user in the Entrust IdentityGuard Server protecting the domain. Unregistered users may be treated differently (see [“Users without Entrust IdentityGuard” on page 69](#)).
- 2 Clicking the arrow icon brings the user to the second-factor authentication screen. The type of second-factor authentication depends on the user's

configuration in Entrust IdentityGuard. The following example shows a grid challenge.



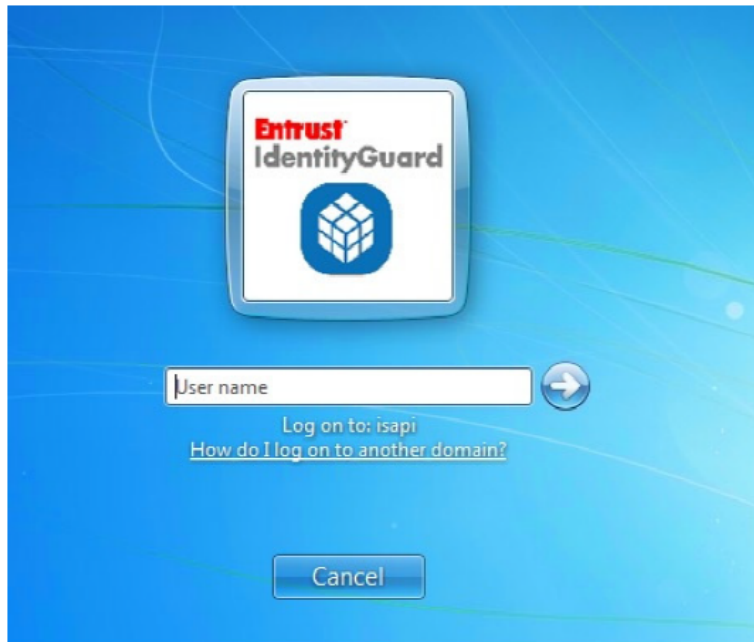
**Note:**

After the user clicks the arrow button and the second-factor authentication screen appears, they cannot return to the first-factor login screen. If the user decides to back-out of second-factor authentication without completing the challenge, they must use the **Switch User** button.

- 3** The user provides the response to the second factor challenge and then clicks the arrow to complete the authentication process.
- 4** When passwordless authentication is set, the next time the user logs in, the user needs only to provide their user name (as shown in the screenshot below) and



then clicks the arrow to proceed to second factor authentication as defined by the user's configuration in Entrust IdentityGuard.



- 5 The user provides the response to the second factor authentication and then clicks the arrow to complete the authentication process.

## Online Question and Answer (Q&A)

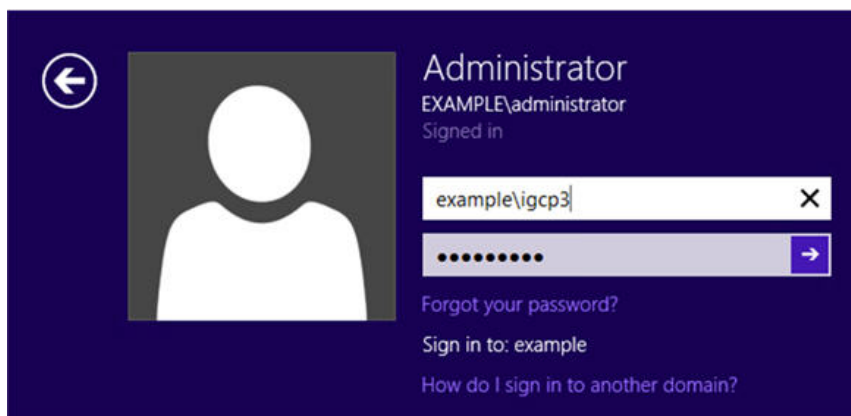
Before Q&A can be configured for use on the user's computer, the user's profile on the Entrust IdentityGuard Server must have Q&A set up and the minimum number of challenges must be configured. This can be done using Entrust IdentityGuard Self-Service Module or directly on the Entrust IdentityGuard Server.

See the *Entrust IdentityGuard Server Administration Guide* for more information.

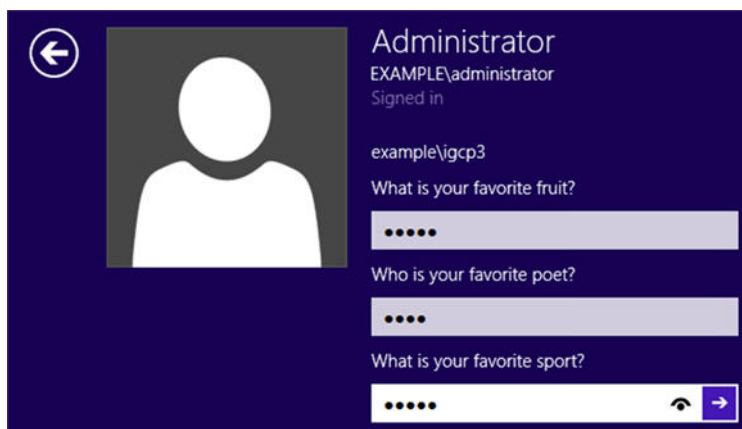
Like any authentication method, Q&A must be set up online (allowing the challenge to be saved locally) before it can be used offline.

### To set up Q&A

- 1 The user log in and successfully complete first-factor authentication.



- 2 At the second-factor authentication screen, the Q&A challenge is presented to the user.



- 3 The user must respond successfully to the challenge, Entrust IdentityGuard validates the entered values and authenticates the user.
- 4 If all responses are correct, the questions and answers are stored locally for later offline use.

## Offline Question and Answer (Q&A)

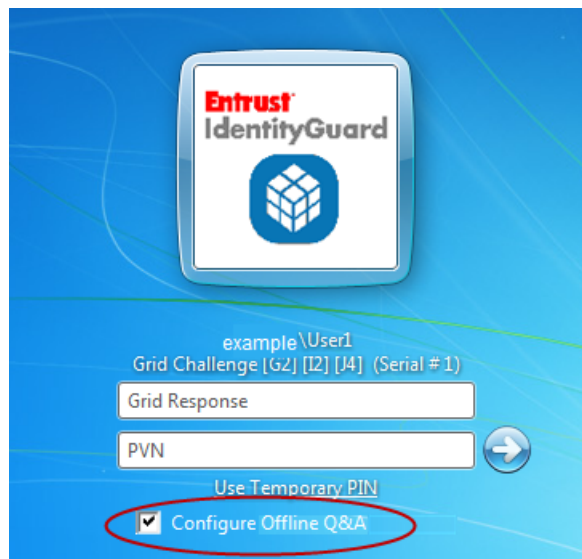
Before Q&A can be configured for offline use on the user's computer, the user's profile on the Entrust IdentityGuard Server must have Q&A set up and the minimum number of challenges must be configured. This can be done using Entrust IdentityGuard Self-Service Module or directly on the Entrust IdentityGuard Server. See the *Entrust IdentityGuard Server Administration Guide* for more information.

To configure Q&A for offline use as a user option in your Desktop for Windows package, select it when you configure the Entrust IdentityGuard Desktop for Windows installation package. See ["Using the custom installation wizard" on page 84](#).

Like any offline authentication method, Offline Q&A must be set up online (allowing the challenge to be saved locally) before it can be used offline.

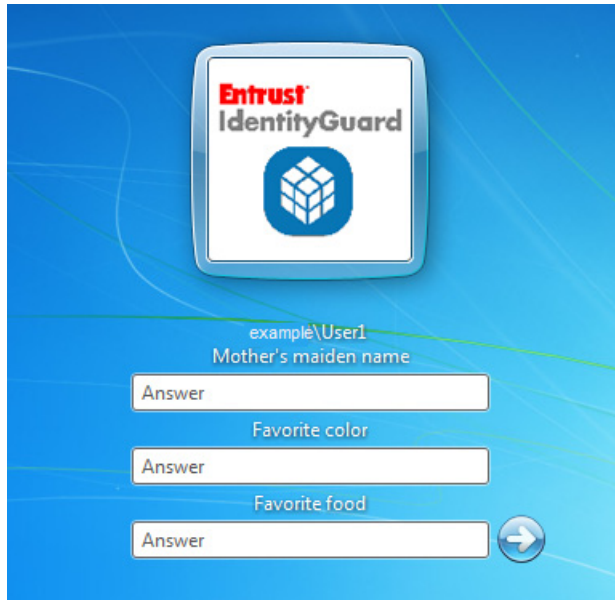
### To set up Q&A for offline use

- 1 Logging in online, the user completes first-factor authentication successfully.
- 2 At the second-factor authentication screen, the user selects **Configure Offline Q&A** before completing the challenge.



A query is made to Entrust IdentityGuard to verify that the user has Q&A enabled and a challenge is ready for that user.

- 3 The Q&A challenge is presented to the user.



The user must respond successfully to the challenge. If all responses are correct, the questions and answers are stored locally for later offline use.



**Note:**

If the user hits the escape button at this time, or fails to respond correctly to the Q&A challenge from Entrust IdentityGuard, no Q&A pairs are stored locally. Any previous Q&A pairs are kept.

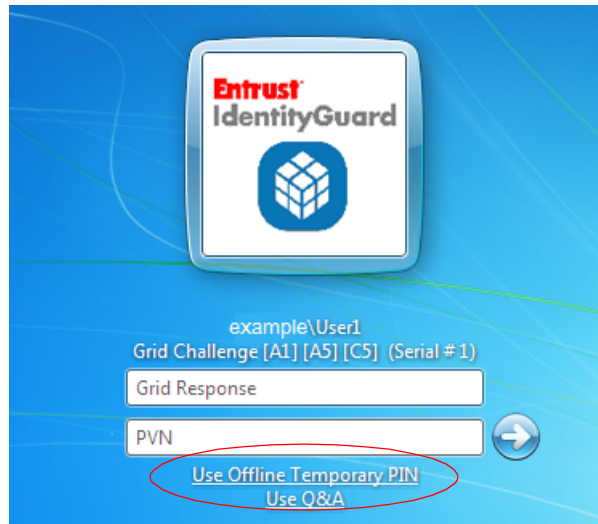
Failing the challenge uses up one of the users authentication attempts. Too many failed attempts could cause the user to be locked out.

If the user updates their Q&A in Entrust IdentityGuard, they can check **Configure or Update Offline Q&A** the next time they log in online, and the same steps taken previously to set the Q&A are executed again.

**To log in offline using Q&A**

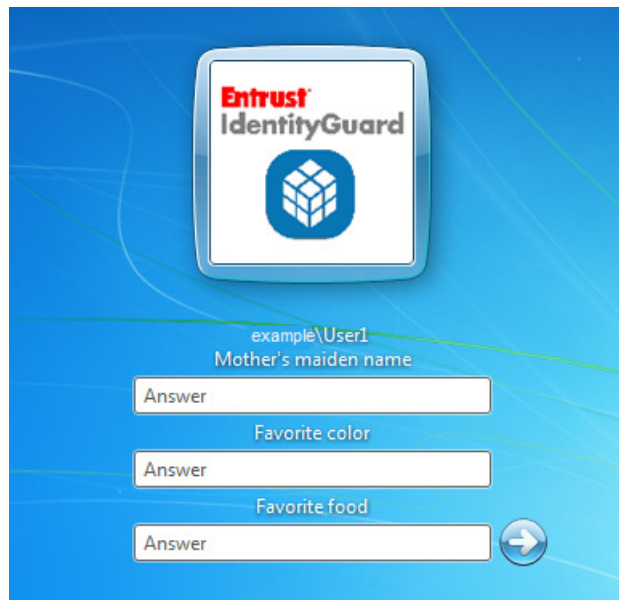
- 1 The user completes first-factor authentication successfully.

- 2 The user selects **Use Q&A** from the second-factor authentication screen.



The screenshot shows the Entrust IdentityGuard authentication interface. At the top is the Entrust IdentityGuard logo. Below it, the user is identified as 'example\User1' and a 'Grid Challenge [A1] [A5] [C5] (Serial # 1)' is displayed. There are two input fields: 'Grid Response' and 'PVN'. To the right of the 'PVN' field is a blue circular button with a white right-pointing arrow. Below the 'PVN' field, two options are listed: 'Use Offline Temporary PIN' and 'Use Q&A'. The 'Use Q&A' option is circled in red.

- 3 The user enters the correct responses in the **Answer** fields.



The screenshot shows the same Entrust IdentityGuard authentication interface, but now the 'Use Q&A' option has been selected. The 'Grid Challenge' is still present. Below the 'PVN' field, the 'Answer' fields are now visible. There are three 'Answer' input fields, each with a label to its right: 'Mother's maiden name', 'Favorite color', and 'Favorite food'. A blue circular button with a white right-pointing arrow is located to the right of the third 'Answer' field.

**Note:**

All answers must be exact. For example, if the answer includes the word `doctor` you must use word `doctor`, not `Dr` . Unlike Entrust IdentityGuard Server, Entrust IdentityGuard Desktop for Microsoft Windows does not support word substitution.

---

## Offline token

Before token authentication can be configured for offline use on the user's computer, the user's profile on the Entrust IdentityGuard Server must have offline token set up. This can be done using Entrust IdentityGuard Self-Service Module or directly on the Entrust IdentityGuard Server. See the *Entrust IdentityGuard Server Administration Guide* for more information.

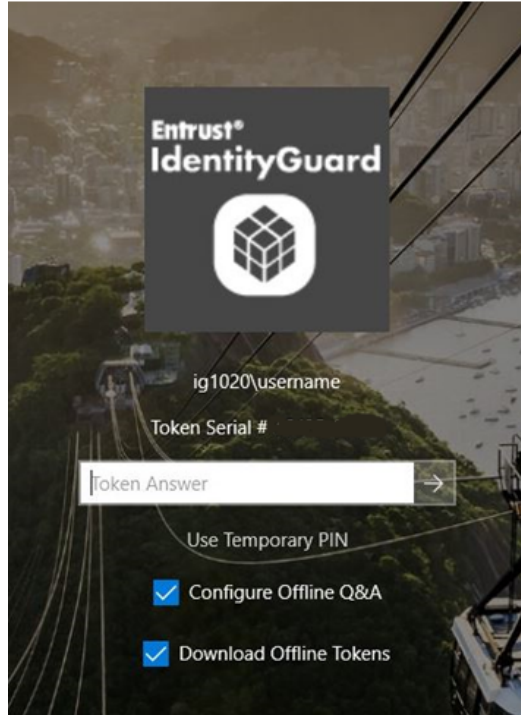
To configure token authentication for offline use as a user option in your Desktop for Windows package, select offline token authentication when you configure the Entrust IdentityGuard Desktop for Windows installation package. See ["Using the custom installation wizard" on page 84](#).

Like any offline authentication method, Offline token must be set up online (allowing the challenge to be saved locally) before it can be used offline.

### To set up token authentication for offline use

- 1 Logging in online, the user completes first-factor authentication successfully.

- 2 At the second-factor authentication screen, the user enters the Token response (and PVN, if configured) and selects the **Download Offline Tokens** checkbox..



Entrust®  
IdentityGuard

ig1020\username

Token Serial #

Token Answer →

[Use Temporary PIN](#)

☒ Configure Offline Q&A

☒ Download Offline Tokens

**Note:**

The Default Offline OTP hours downloaded for the first time is the hours configured in the Entrust IdentityGuard registry setting, for example, 24 hours..

On Consecutive logins, if the user does not check the **Download Offline Tokens** checkbox, the minimum number of hours configured in Entrust IdentityGuard Server is downloaded, for example, 1 hour.

If the user checks the **Download Offline Tokens** checkbox, the The Offline OTP hours downloaded are based on the Max number of hours configured in the Entrust IdentityGuard Server, for example, 16 hours.

In addition, the **Protected Offline OTP Max Client** policy setting also sets the number of machines to which a user can download offline tokens.

For example:

If **Protected Offline OTP Max. Client** = 1, then the user can download the offline token only on one machine.

If **Protected Offline OTP Max. Client** = 10, then the user can download the offline token on 10 machines.

- 
- 3** A query is made to Entrust IdentityGuard to verify that the user has Token enabled and a challenge is ready for that user.
  - 4** The user must respond successfully to the challenge. If all responses are correct, the tokens are stored locally for later offline use.

**Note:**

Failing the challenge uses up one of the users authentication attempts. Too many failed attempts can cause the user to be locked out.

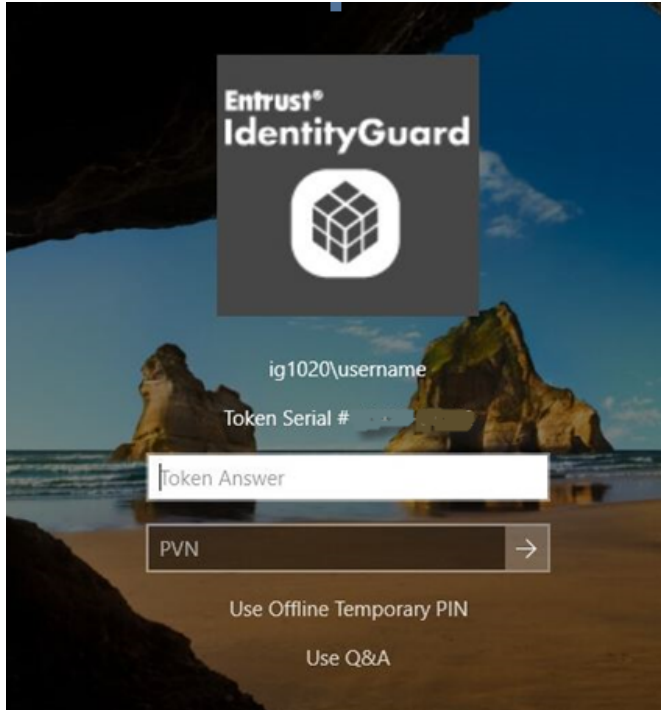
- 
- 5** To update the offline OTPs, the user must repeat this procedure while online.

**To log in offline using OTP**

- 1** The user completes first-factor authentication successfully.



- 
- 2 The user responds with the OTP and PVN (If configured) on second-factor authentication page.



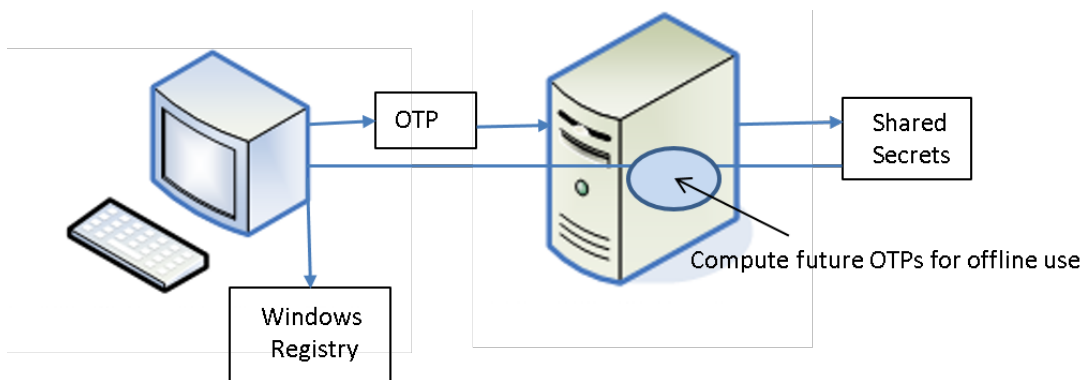
- 
- 
- 3 The user clicks **Submit**.

## How the offline token works

When a user authenticates to the Entrust IdentityGuard Server for using an OTP, if configured for offline token, the Windows Desktop client login window includes a check box to download offline tokens.

If the user selects to download offline tokens, a collection of OTPs for that token are generated by the Entrust IdentityGuard Authentication server, and a keyed hash of the OTPs are sent back to be stored in the Windows desktop registry on the user's computer. The number of available OTPs and their lifetime is determined by the policy settings in Entrust IdentityGuard Server along with the number of hours that offline login with OTP is permitted on the Windows Desktop client.

When the user wants to log in offline, they use an OTP that has been stored in the Windows Desktop registry.



After the initial login and download of offline OTPs, if the download offline tokens option is unchecked on the login page, subsequent logins download offline OTPs for Minor Hours (according to the policy setting in Entrust IdentityGuard Server).

If the download offline token is checked, it downloads OTPs for Max Hours (according to policy setting in Entrust IdentityGuard Server).

## Personal verification numbers

The personal verification number (PVN) feature provided with Entrust IdentityGuard lets you add 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; 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, they will receive the request the next time they log on. The change request appears with the second-factor challenge.

The screenshot shows the Entrust IdentityGuard login interface. At the top is the Entrust IdentityGuard logo. Below it, the text "example\User1" is displayed. A "Grid Challenge [G5] [I2] [J3] (Serial # 27)" is presented. There are four input fields: "Grid Response", "PVN", "New PVN", and "Confirm New PVN". A blue arrow button is to the right of the "Confirm New PVN" field. At the bottom, there is a link that says "Use Temporary PIN".

## Temporary PIN authentication

In certain situations, where the user does not have a grid or token, you can issue a temporary PIN, either for a specific number of uses or a limited period of time. Examples of this situation include lost grids or tokens, or a newly registered user waiting for their grid or token to arrive.

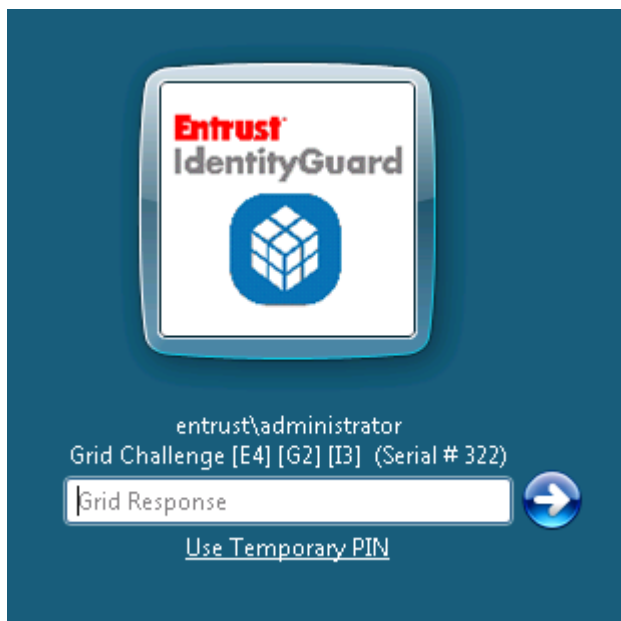
Temporary PINs are configured on the Entrust IdentityGuard Server. Administrators issue the temporary PINs to users, and can limit their use based on time or number of uses. When configuring the limits, administrators must consider the length of time it takes to deliver a replacement grid or token to the user.



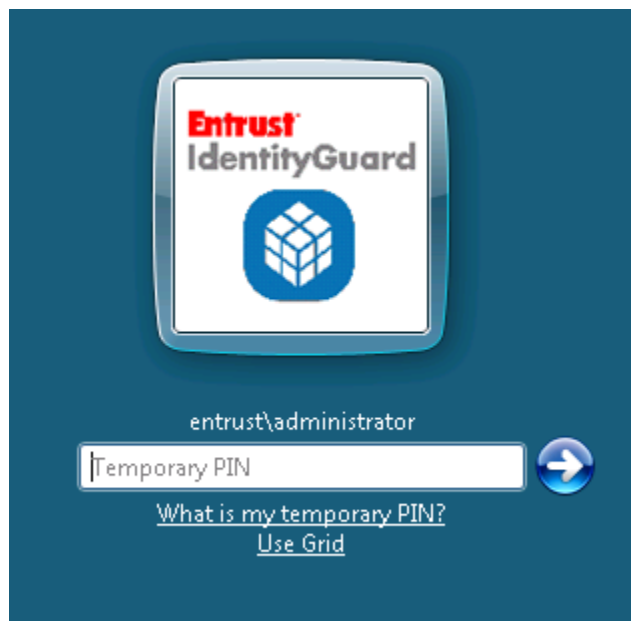
### Note:

If you do not want to offer users the option to log in with a temporary PIN, you can hide this link. For more information, see [EnableOnlineTempPINAuth](#) in "Registry settings under 'WIGL'" on page 147.

To access the temporary PIN screen, the user clicks **Use temporary PIN**.



If the user clicks **Use temporary PIN**, Entrust IdentityGuard displays the following screen.



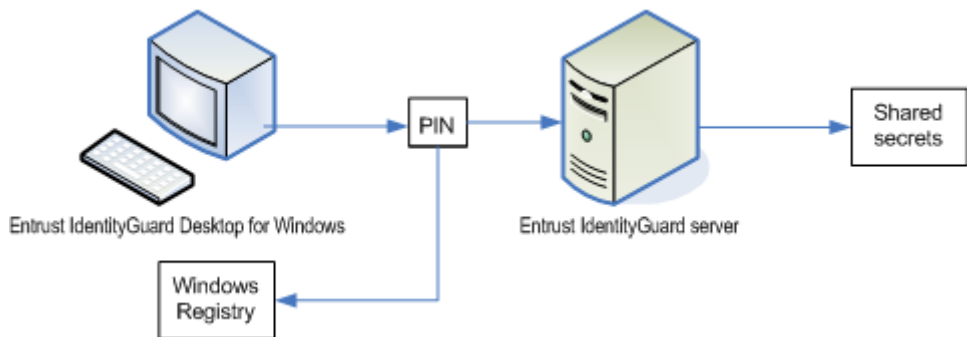
When the user enters the correct temporary PIN, the user is able to access their desktop. If the user enters an incorrect temporary PIN, the server counts the number of attempts and locks the user out after a limit is reached. The number of allowable attempts is configured at the Entrust IdentityGuard Server. See the *Entrust IdentityGuard Administration Guide* for further information.

When the user clicks **What is my temporary PIN?**, Entrust IdentityGuard Desktop for Microsoft Windows displays a message telling the user how to get a temporary PIN. (See [“To create a custom installation package” on page 84](#) for more information about customizing this message.)

You can require your users to use a personal verification number (PVN) with the temporary PIN for additional security. See [“Personal verification numbers” on page 58](#).

### How the offline temporary PIN works

When a user authenticates to the Entrust IdentityGuard Server for the first time, either with a challenge and response or an online temporary PIN, the Entrust IdentityGuard Windows Desktop client generates an offline temporary PIN for the user's computer.



The offline temporary PIN is saved at the Entrust IdentityGuard Authentication server on the user's **Account Information** page (in the Entrust IdentityGuard Administration interface) under **Shared Secrets**, and a keyed hash of the PIN is stored in the Windows desktop registry on the user's computer.

The user uses this offline temporary PIN for this particular computer in the future. If the last login also included a PVN, the PVN is saved for offline use.

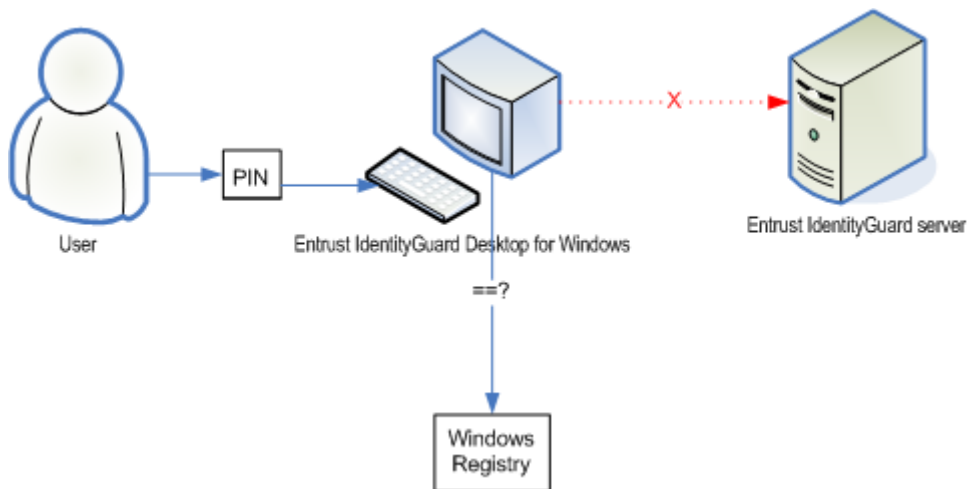
When the user wants to log in offline, they contact an Entrust IdentityGuard administrator. The administrator looks up the offline temporary PIN and communicates the PIN to the user. The PIN is stored in the user's shared secrets and looks similar to:

```
IGWOfflinePIN_RLEESP = 2T3D8NPV
```

where RLEESP is the computer name and 2T3D8NPV is the offline temporary PIN value. Users that have authenticated online from multiple computers have multiple shared secrets. The administrator must choose the correct one based on the computer the user is logging on to.



To use their offline temporary PIN, users can click **Use offline temporary PIN** in the Entrust IdentityGuard Authentication login screen. The user enters the offline PIN into the Entrust IdentityGuard Windows Desktop client. The client compares the PIN value with the value stored in the registry. If they match, the user is permitted to log in to the computer.



The next time the user logs in online, Entrust IdentityGuard creates a new offline temporary PIN for the computer. The user must use this new offline temporary PIN the next time they log in offline with a temporary PIN.

For information about configuring offline temporary PINs, see ["Configuring authentication options" on page 77](#).

**Note:**

If you delete a user in the Entrust IdentityGuard Server, the offline PINs will be lost. Because of this, if you delete and recreate the same user in Entrust IdentityGuard, the new user will not be able to log in offline using a temporary PIN. Before deleting a user from Entrust IdentityGuard, record or save their shared secret.

---

# Biometric enrollment with the fingerprint enrollment client

This section describes the user experience of installing the Entrust IdentityGuard Desktop for Microsoft Windows client and the fingerprint enrollment client, and then using the fingerprint enrollment client to enroll fingerprints for biometric authentication.

## Prerequisites

- A fingerprint scanner must be connected to the user's computer to complete fingerprint enrollment.
- The Entrust IdentityGuard administrator must move the biometric authentication to the top of the auth types list in the Entrust IdentityGuard server admin URL (see ["Accessing the biometric self-service module enrollment page" on page 64](#)).

## Accessing the biometric self-service module enrollment page

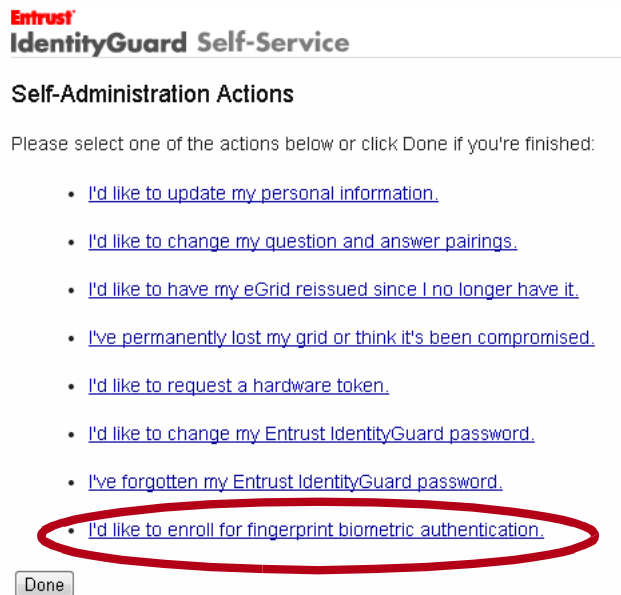
The following process explains how to prepare Entrust IdentityGuard for biometric enrollment with fingerprint.

### Prepare for biometric enrollment

- 1 The administrator installs Entrust IdentityGuard and completes the normal configuration.
- 2 The administrator creates a group policy selects the following:  
**Normal Security Authentication Types: Biometric, OTP**
- 3 The users accesses Entrust IdentityGuard Desktop for Windows and enters their password.
- 4 Entrust IdentityGuard Desktop for Windows validates the password and caches it.
- 5 Entrust IdentityGuard Desktop for Windows then asks Entrust IdentityGuard for the authenticator.
- 6 Entrust IdentityGuard requests a one-time password (OTP) because biometric is not yet registered for the user.
- 7 The user enters their OTP, logs into Self-Service Module and enrolls their fingerprint.
- 8 The user locks their computer.
- 9 The user logs in to their computer.
- 10 Entrust IdentityGuard Desktop for Windows asks Entrust IdentityGuard for the authenticator.



- 11 Entrust IdentityGuard responds that biometric authentication is required because the user has enrolled their biometric.
- 12 The user authenticates with their finger.
- 13 Entrust IdentityGuard Desktop for Windows validates with Entrust IdentityGuard and the user logs in.
- 14 The user logs in to Self-Service with a user name and password. If the user has not previously registered with Entrust IdentityGuard, the Web application leads them through the registration process.
- 15 After logging in and registering, the **Self-Administration Actions** page appears.



- 16 The user clicks **I'd like to enroll for fingerprint biometric authentication.**

An enrollment page appears.

## **Entrust** **IdentityGuard Self-Service**

### **Enroll For Fingerprint Biometric Authentication**

To enroll for fingerprint biometric authentication, close any existing instance of the Entrust IdentityGuard Fingerprint Enrollment client, and select the **Fingerprint Data** button below.

#### **Capture Fingerprint Data**

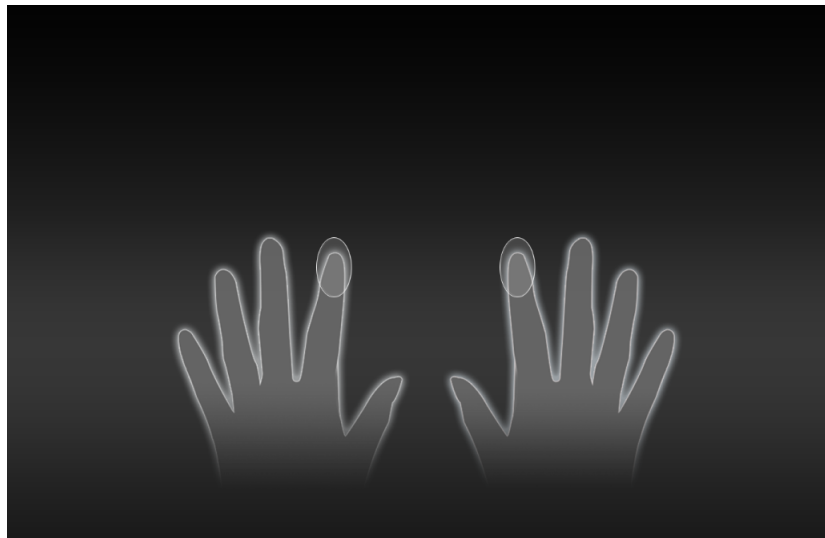
Once the program launches, you must ensure that at least one fingerprint is captured. For more detailed instructions that are specific to your work contact a System Administrator for assistance.

Once your fingerprint data has been collected, and the Entrust IdentityGuard Fingerprint Enrollment client has closed, return here and select **Next**.

If you run into any problems, or don't want to enroll for fingerprint biometric authentication at this time, select **Cancel**.

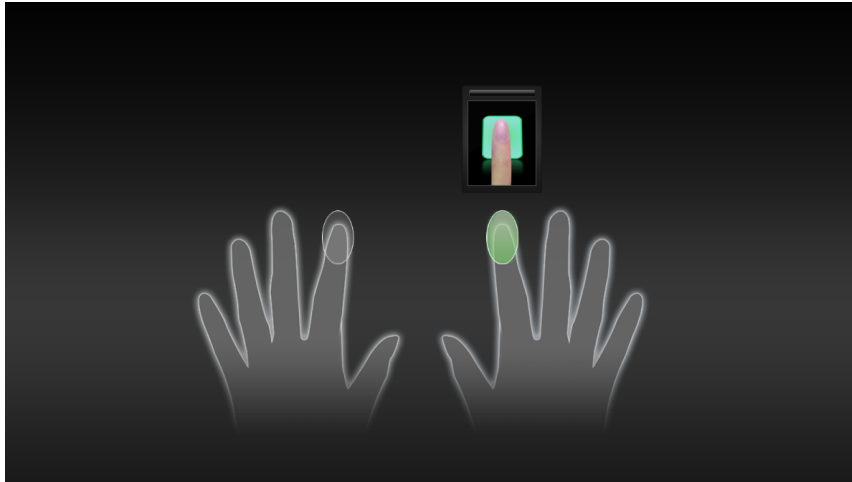
#### **17** The user clicks **Capture Fingerprint Data**.

A green light appears on the fingerprint scanner. After a few seconds, the fingerprint enrollment client appears on the user's Windows desktop.

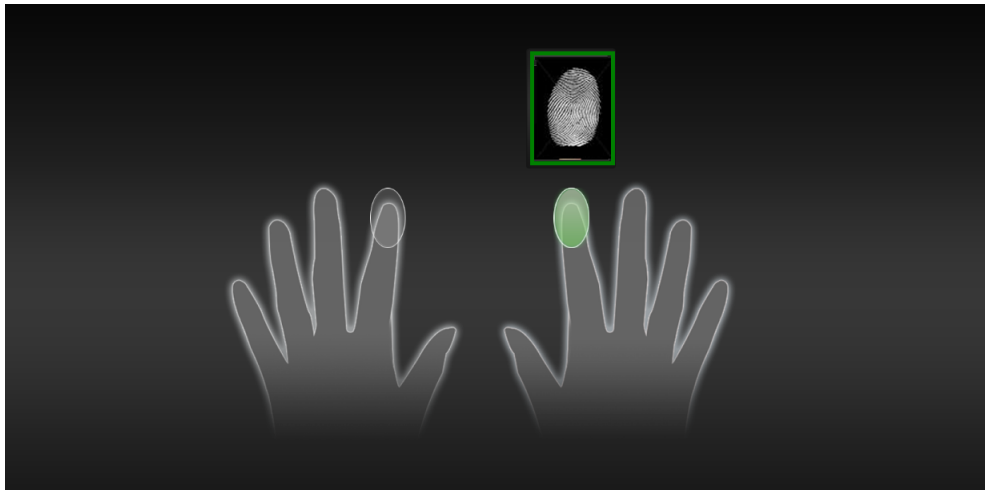


#### **18** The user clicks the image of the finger for which to enroll a fingerprint. The fingers that are circled are recommended, however, users can enroll any fingerprints they choose, or those specified by a system administrator.

A green circle appears around the finger selected.

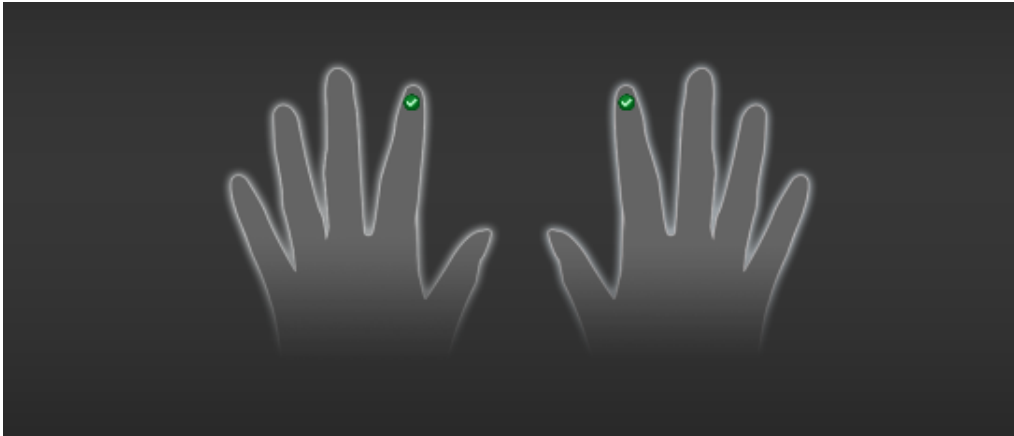


- 19** The user places and holds that finger on the fingerprint scanner until a green box appears around the fingerprint image.



- 20** The user repeats this scanning procedure two more times with the same finger.
- 21** The user clicks a different finger in the software and repeat the fingerprint scan three times for the next selected finger.
- 22** When the user has scanned two fingerprints (or the number required by your organization), the user clicks **Next**.

A success message appears, indicating the required fingerprints are enrolled.



- 23** The user clicks **Finish** and is returned to the Self-Service page.
- 24** The user clicks **Next**, and then **Done** to complete the enrollment process.  
The user has now enrolled fingerprints to be used for biometric authentication.

# Users without Entrust IdentityGuard

Users who do not have Entrust IdentityGuard user IDs, and who log into a Microsoft Windows client computer with Entrust IdentityGuard installed, may be blocked from access to the desktop, depending on how you configured the Entrust IdentityGuard Desktop for Microsoft Windows installation package.

For more information, see [“Configuring authentication options” on page 77](#).

Unregistered users can have access to a computer with Entrust IdentityGuard Desktop for Microsoft Windows installed. This allows Entrust IdentityGuard users and non-Entrust IdentityGuard users to use the same computers, but not have access to the same data. It also lets you deploy Entrust IdentityGuard Desktop for Microsoft Windows before you add users to Entrust IdentityGuard.



**Note:**

Local accounts never require Entrust IdentityGuard authentication.

---



# Installing and configuring Entrust IdentityGuard Desktop for Microsoft Windows

Installing and configuring the Windows Login feature of Entrust IdentityGuard Desktop for Microsoft Windows involves pre-installation steps, selecting features to include in the installation package, gathering custom installation data, selecting methods of deployment, and distributing the installation package to your users.

This chapter contains the following topics:

- [“Preparing for installation” on page 72](#)
- [“Understanding Desktop for Microsoft Windows settings” on page 75](#)
- [“Customizing the Entrust IdentityGuard Desktop for Microsoft Windows installation package” on page 83](#)
- [“Testing the installation package” on page 107](#)
- [“Providing the installation package as an executable or as a Windows Installer file” on page 108](#)
- [“Distributing the installation package” on page 109](#)
- [“Creating an administrative installation” on page 113](#)
- [“Saving the offline registry key when upgrading” on page 119](#)

# Preparing for installation

The following sections outline the steps you must take to prepare to install Entrust IdentityGuard Desktop for Microsoft Windows.

- [“Setting up users” on page 72](#)
- [“Gathering custom installation data” on page 73](#)
- [“Communication between Desktop for Microsoft Windows and the Entrust IdentityGuard Server” on page 73](#)

## Setting up users

Users must have user IDs in the network and be configured on the Entrust IdentityGuard Server before they can use Entrust IdentityGuard Desktop for Microsoft Windows. The pre-installation and installation sequence is:

- An administrator creates user IDs for users.
- An administrator creates grids in Entrust IdentityGuard (if applicable).
- An administrator assigns a grid, token, PVN or temporary PIN to each user, as required by your configuration.
- An administrator instructs users to register for knowledge-based authentication using Self-Service Module or some other method. (Offline users can authenticate using a Q&A challenge.)
- Administrators create a customized installation package and deploy it to users.
- Users install the customized installation package on their Windows desktop. To use biometric authentication, users install the fingerprint enrollment client from the same installation package.



### **Note:**

If you are using biometric authentication, advise users that they must complete enrollment of their fingerprint data in the same Windows session as when they install the fingerprint enrollment client. If a user locks the Windows computer (or if it locks automatically after a period of inactivity) before fingerprint data is enrolled, the user may not be able to log in to the computer.

---



## Gathering custom installation data

Collect custom installation data related to your organization's Entrust IdentityGuard setup. Use the worksheets in ["Customizing the installation package" on page 135](#) to plan the data required for your Entrust IdentityGuard Desktop for Microsoft Windows deployment.

## Communication between Desktop for Microsoft Windows and the Entrust IdentityGuard Server

The Entrust IdentityGuard Server implements a Web service for authentication using HTTPS. During configuration, you are asked for the URL of the authentication service running on the Entrust IdentityGuard Server.

This URL can be obtained from the Entrust IdentityGuard Server's Web service and Application Manager interface (accessed through the Entrust IdentityGuard Configuration Panel).

The format of the URL is as follows:

```
https://ig.example.com:8443/IdentityGuardAuthService/services/Auth  
enticationServiceV11
```



### **Note:**

Entrust IdentityGuard Desktop for Windows version 12 requires the V11 authentication service that is part of Entrust IdentityGuard Server version 12 and later. To check that you are using the latest version of the V11 Authentication Service, open the Entrust IdentityGuard Administration interface and ensure that the software version number at the bottom of the page is 12 or later.

To establish secure SSL communication between the server and Entrust IdentityGuard Desktop for Windows client, client computers must have the trusted root certificate from the Entrust IdentityGuard Server installed in their the local Microsoft certificate store.

When you create the custom installation package, you can add this certificate to the installation package. The certificate (and any others you specify) are installed on the client computer during installation. See ["Customizing the Entrust IdentityGuard Desktop for Microsoft Windows installation package" on page 83](#).

The Entrust IdentityGuard Server may use one of several types of root certificates (see the *Entrust IdentityGuard Installation Guide* for more information):

- a publicly-trusted SSL certificate such as a certificate from Entrust Certificate Services.  
<https://www.entrustdatacard.com/products/categories/ssl-certificates>
- a privately-trusted SSL certificate—for example from a private Certification Authority (CA) used by your network
- a self-signed certificate



**Attention:**

Using a self-signed certificate is not recommended for large deployments. Self-signed certificates are unmanaged, and will expire after a time. When a self-signed certificate expires, it is no longer trusted, and each user desktop must be updated with a new certificate. If the certificate expires, Entrust IdentityGuard Desktop for Microsoft Windows behaves as if Entrust IdentityGuard is not available.

Instead, use an SSL certificate issued by a public root. That way, each time the SSL certificate used by Entrust IdentityGuard expires and is replaced, you do not need to update the Microsoft desktop, because the CA certificate is still trusted.

---

# Understanding Desktop for Microsoft Windows settings

The Windows Login feature has many mandatory and optional settings that you can configure through the **Entrust IdentityGuard Desktop for Microsoft Windows Custom Installation** wizard. Read this section to understand the settings and make decisions about the feature you want to use before you create the desktop installation package with the custom installation wizard discussed in [“To create a custom installation package” on page 84](#). Topics in this section include:

- [“Configuring the Entrust IdentityGuard Server settings” on page 75](#)
- [“Configuring the Self-Service Module settings for password reset” on page 75](#)
- [“Specifying other allowed Credential Providers” on page 76](#)
- [“Including additional certificates” on page 76](#)
- [“Disabling revocation checking” on page 76](#)
- [“Configuring the group type” on page 77](#)
- [“Configuring authentication options” on page 77](#)
- [“Customizing temporary PIN instructions” on page 78](#)
- [“Configuring offline authentication options” on page 78](#)
- [“Customizing the logo on the login screen” on page 80](#)

## Configuring the Entrust IdentityGuard Server settings

You must configure the Entrust IdentityGuard Server information on the **Specify Entrust IdentityGuard Server Information** page in the **Entrust IdentityGuard Desktop Custom Installation** wizard. This information enables the Windows Login feature to communicate securely with the Entrust IdentityGuard Server for second-factor authentication. You can configure multiple Windows domains with multiple Entrust IdentityGuard Servers. Set up communication with the Entrust IdentityGuard Server using HTTPS (not HTTP).

## Configuring the Self-Service Module settings for password reset

If you want users to be able to reset their Windows password and perform other administrative tasks in the Entrust IdentityGuard Self-Service Module, you must complete the following configuration tasks:

- 1 Enable password reset on the Self-Service Module. For more information, see *“Enabling password reset”* in the *Entrust IdentityGuard Self-Service Module Installation and Configuration Guide*.

- 2 Use the Entrust IdentityGuard Desktop for Windows installer customization wizard to
  - enable the option that inserts a link on the Windows login page
  - specify the domain name and URL of one or more SSM instances in your deployment

These steps are described in [“To create a custom installation package” on page 84](#).

## Specifying other allowed Credential Providers

You can choose one or more credential providers to coexist with the Entrust IdentityGuard credential provider. This can allow users to log on using Entrust IdentityGuard credential provider as well as the Microsoft Smart Card credential provider or any other third-party credential provider.

## Including additional certificates

The Microsoft Windows desktop must have a trusted Certificate Authority (CA) root certificate for the Windows Login feature to communicate with the Entrust IdentityGuard Server for second-factor authentication. If the Entrust IdentityGuard Server is not using a self-signed SSL certificate, the trusted CA root certificate that issued Entrust IdentityGuard’s SSL certificate must be imported into the local Microsoft certificate store on the Microsoft Windows desktop. If your users do not currently have the trusted CA root certificate located in their Microsoft certificate stores, you can include this additional certificate in the custom installation package.

## Disabling revocation checking

The Windows Login feature uses the Microsoft Windows revocation checking ability to verify SSL certificates. If Microsoft Windows cannot locate a Certificate Revocation List (CRL), the SSL certificate is rejected.

The Windows Login feature includes a `DisableSSLRevocationChecking` registry setting that allows you to disable revocation checking. You may need to disable revocation checking if the CA that issued the Entrust IdentityGuard Server certificate does not publish its revocation list in a location or format that Microsoft Windows can access.

The `DisableSSLRevocationChecking` setting with a value type `REG_DWORD` must be manually configured in the following location in the Microsoft Windows registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL
```

or

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Entrust\WIGL
```

To disable revocation checking, set `DisableSSLRevocationChecking` to 1 or greater. If this value is missing or is set to 0, certificate revocation checking is performed.

For further information about configuring the `DisableSSLRevocationChecking` setting, see the **Specify Additional Registry Values** page of the custom installation wizard in [“To create a custom installation package” on page 84](#).

## Configuring the group type

An Entrust IdentityGuard group organizes users, grids, and tokens. You can assign different policies to different groupings of users and grids (or tokens).

When the Windows desktop user attempts to communicate with the Entrust IdentityGuard Server for second-factor authentication, the group type configured at the Windows desktop must match the group type configured at the Entrust IdentityGuard Server.

Configure the group type on the **Configure Group Type** page in the **Entrust IdentityGuard Desktop Custom Installation** wizard. You can configure one of the following group types:

- **Group determined by Entrust IdentityGuard Server**—use this selection when you are not using IdentityGuard groups, or your user names are unique across all IdentityGuard groups.



### Attention:

Do not use this selection if any of your users' names are not unique. This causes Entrust IdentityGuard authentication to fail for the user.

---

- **Use Windows domain as Entrust IdentityGuard group**—use this selection when the user's group name is the same as the Windows domain name.
- **Use this group**—use this selection when you know the group name. Enter the group name in the text box.

## Configuring authentication options

You can configure the Windows Login feature to force users who are accessing and unlocking their Windows desktop computer to use Entrust IdentityGuard authentication.

You can configure the following authentication options in the **Configure Windows Login Options** page in the **Entrust IdentityGuard Custom Installation** wizard:

- **Authentication to Entrust IdentityGuard is mandatory**
- **Authentication to Entrust IdentityGuard when computer is being unlocked**
- **Enable Q&A for offline authentication**

## Customizing temporary PIN instructions

You can assign a temporary PIN to a Windows Login user when a grid or token is lost or forgotten. The user can then authenticate without the grid (or token) for a specified period of time or number of uses. The temporary PIN becomes invalid at a specified expiry time, or after a certain number of uses, or when the current grid (or token) is used.

You can configure the Windows Login feature to display customized instructions for the user to tell them how to obtain or use a temporary PIN. You can customize two messages, one for temporary PIN, and one for offline temporary PIN. If you do not provide a message, the default message is used.

The Windows Login feature displays the appropriate customized message when users click the following links on the **Entrust IdentityGuard** credential provider screen:

- **What is my temporary PIN?**
- **What is my offline temporary PIN?**

## Configuring offline authentication options

The Windows Login feature tries to authenticate users in offline mode whenever the user's computer is not connected to the network, or the Entrust IdentityGuard Server is not available.

The Windows Login feature saves a number of grid and token challenge sets and the corresponding hash values based on the correct response for each user in the registry, when users authenticate them online. The hash is computed securely from the valid response and the valid response is not saved.

When the server is unavailable, Entrust IdentityGuard Desktop for Microsoft Windows retrieves one of the saved challenge sets and the corresponding hash and then presents the challenge set to the user. After the user provides the response, Desktop for Microsoft Windows computes the hash based on the response. If the computed hash matches the saved hash value, the user is allowed to log in.

If there are no challenge sets saved for that user in the registry, (for example, if the user has never successfully authenticated to the Entrust IdentityGuard Server online) then the user is treated as a non-Entrust IdentityGuard user.

You can configure the number of challenge responses that are saved for authentication by changing the value in the `OfflineChallengeResponseCount`

setting. If the value in `OfflineChallengeResponseCount` is zero or missing, the default value 5 is used. `OfflineChallengeResponseCount` is located in the registry, under `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL`.

## Specifying the maximum offline challenge attempts

When you are customizing the **Entrust IdentityGuard Desktop Custom Installation** wizard, you can configure the Windows Login feature to lock out a user after a maximum number of challenge attempts while the user is offline.

Configure the **Max number of challenge attempts after which computer is locked out** setting on the **Configure Windows Login Offline Options** page in the **Entrust IdentityGuard Desktop Custom Installation** wizard. By default, the maximum number of challenge attempts is set to 5. Specifying the maximum offline temporary PIN attempts

When you are customizing the **Entrust IdentityGuard Desktop Custom Installation** wizard, you can configure the Windows Login feature to lock out a user after a maximum number of temporary PIN attempts while the user is offline.

Configure the **Max number of temporary PIN attempts after which computer is locked out** setting on the **Configure Windows Login Offline Options** page in the **Entrust IdentityGuard Desktop Custom Installation** wizard. By default, the maximum number of temporary PIN attempts is set to 5.

## Specifying the maximum number of Q&A attempts

When you are customizing the **Entrust IdentityGuard Desktop Custom Installation** wizard, you can configure the Windows Login feature to lock out a user after a maximum number of Q&A attempts while the user is offline.

Configure the **Max number of Q&A attempts after which computer is locked out** setting on the **Configure Windows Login Offline Options** page in the **Entrust IdentityGuard Desktop Custom Installation** wizard. By default, the maximum number of attempts is set to 5.

## Specifying the offline temporary PIN lock-out time

When you are customizing the **Entrust IdentityGuard Desktop Custom Installation** wizard, you can configure the Windows Login feature to prevent a user from using their offline temporary PIN for a specified time limit in minutes.

Configure the setting **The offline temporary PIN lock-out time limit in minutes** on the **Configure Windows Login Offline Options** page in the **Entrust IdentityGuard Desktop Custom Installation** wizard. By default, the time limit is set to 15 minutes.

## Customizing the logo on the login screen

You can replace the Entrust IdentityGuard Desktop logo with their company logo or other image. This image is shown to users on the Windows login screen. This customization is done as part of the desktop installer customization.

The image must be located in a network share accessible to users when they install the desktop client. The path must be in the following format:

`\\<path>\<image_file>.bmp`

The logo image must be in bitmap form (.bmp). The recommended size of the image is 128 X 128 pixels. If the image is smaller or larger, it will be scaled to fit the available space.



### **Note:**

The logo customization and appearance of the logo on the Login screen on Windows 8 and higher is set by the Windows Group Policy.

The logo customization and appearance of the logo on the Login screen is applicable to Windows 7 and Windows 2008 R2.

---



# About Microsoft Windows Installer

Microsoft Windows Installer is based on a data-driven model, and provides all installation data and instructions in a single, complete package (MSI file and any external source files that are referenced by this file). Double-clicking an MSI file invokes the Windows Installer service.

You can customize a Windows Installer file by applying a transform (MST file)—a collection of changes applied to a base MSI file. You apply a transform as part of an initial installation. You cannot apply a transform file to an application that is already installed. You can apply multiple transform files to the Windows Installer file to create multiple installation packages for different groups of users.

After the application is successfully installed using the Windows Installer (MSI), the MSI prompts the user to restart the computer to start the Entrust software. A cached version of the original MSI file is maintained on the target computer. To allow for future installation repairs or re-installations, Windows Installer also caches a copy of any transform file used during the installation.

## What is an administrative installation?

An administrative installation decompresses the application files, copies them to a specified network location, and copies an updated Windows Installer package to the same location. Users who have access to the network location can install the image. For more information, see ["Creating an administrative installation" on page 113](#).



### **Note:**

An administrative installation uncompresses the application files, therefore, the administrative installation is larger than the original Windows Installer package (MSI). As a result, the updated Windows Installer package is smaller because it no longer contains any application files. This is expected behavior for a Windows Installer because the uncompressed files cannot be compressed again into a single installer package (MSI).

---

## What is a transform file?

A transform is a collection of specified changes in the form of an MST file that you apply to a base Windows Installer package (MSI) file at installation time. Transforms customize the installation of an application to meet your organization's needs.

## Windows Installer logging

Windows Installer has a built-in logging mechanism that can help identify any installation issues that may occur during the setup. Logging can be enabled through the command-line option, registry-key configuration, or other methods specified in Microsoft documentation.

# Customizing the Entrust IdentityGuard Desktop for Microsoft Windows installation package

Use the **Entrust IdentityGuard Desktop Custom Installation** wizard to create customized Installation packages for users in your organization. The wizard is available in the following location. Use the wizard appropriate for your operating system.

There are two installers, depending on your operating system.

- For Windows 7 and Windows Server 2008 R2 (x86 and x64), use IDG\_CP\_12.0\_win7\_Server2008R2, as follows:
  - For 64-bit: <install folder>\Utilities\eigwincustwiz64.exe
  - For 32-bit: <install folder>\Utilities\eigwincustwiz32.exe
- For Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2016, use IDG\_CP\_12.0\_win81\_Server2016, as follows:
  - For 64-bit: <install folder>\Utilities\eigwincustwiz64.exe
  - For 32-bit: <install folder>\Utilities\eigwincustwiz32.exe

The **Custom Installation** wizard uses a Microsoft Windows Installer file (MSI) provided with the Entrust IdentityGuard Desktop for Microsoft Windows software. The **Custom Installation** wizard creates a transform file (MST), which is a repository of changes to apply to the base MSI file.

Entrust IdentityGuard Desktop for Microsoft Windows is delivered as a Windows Installer package (MSI file) that you can configure.

The Entrust IdentityGuard Desktop for Microsoft Windows ZIP file contains the following file structure in the IG\_Dsktp\_12\_MSWin64 (or IG\_Dsktp\_12\_MSWin32) folder:

- `license.txt`—the Entrust IdentityGuard for Microsoft Windows license.
- `eigdsktp64.msi` (or `eigdsktp32.msi`)—the Entrust IdentityGuard Desktop for Windows and fingerprint enrollment client installer package.
- `setup.ini`—the `setup.exe` configuration file.
- `setup.exe`—the Entrust IdentityGuard Desktop setup executable.
- Utilities folder
  - `eigwincustwiz64.exe` (or `eigwincustwiz32.exe`)—the **Entrust IdentityGuard Desktop for Microsoft Windows Custom Installation** wizard.
  - `AllowCredentialProviders.ini`—the file you use to specify other credential providers that can coexist in your implementation in addition to Entrust IdentityGuard Desktop for Microsoft Windows.

## Using the custom installation wizard

The following procedure describes the steps involved in creating a custom installation package with the **Entrust IdentityGuard Desktop Custom Installation** wizard.

### To create a custom installation package

- 1 On any computer running a supported version of Windows, download and extract the required installation file from Entrust Trustedcare (<https://trustedcare.entrustdatacard.com>).

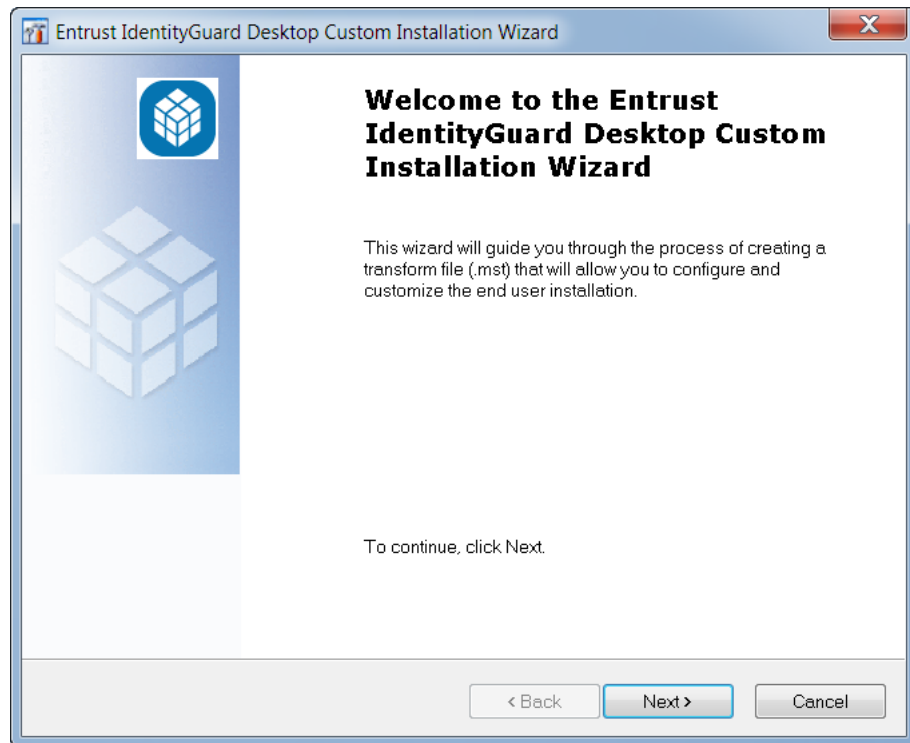
To access the site, use the user name and password provided by your Entrust representative.

- For Windows 7 and Windows Server 2008 R2 (x86 and x64), use IDG\_CP\_12.0\_win7\_Server2008R2
- For Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2016, use IDG\_CP\_12.0\_win81\_Server2016.

- 2 Launch the **Custom Installation** wizard as follows:

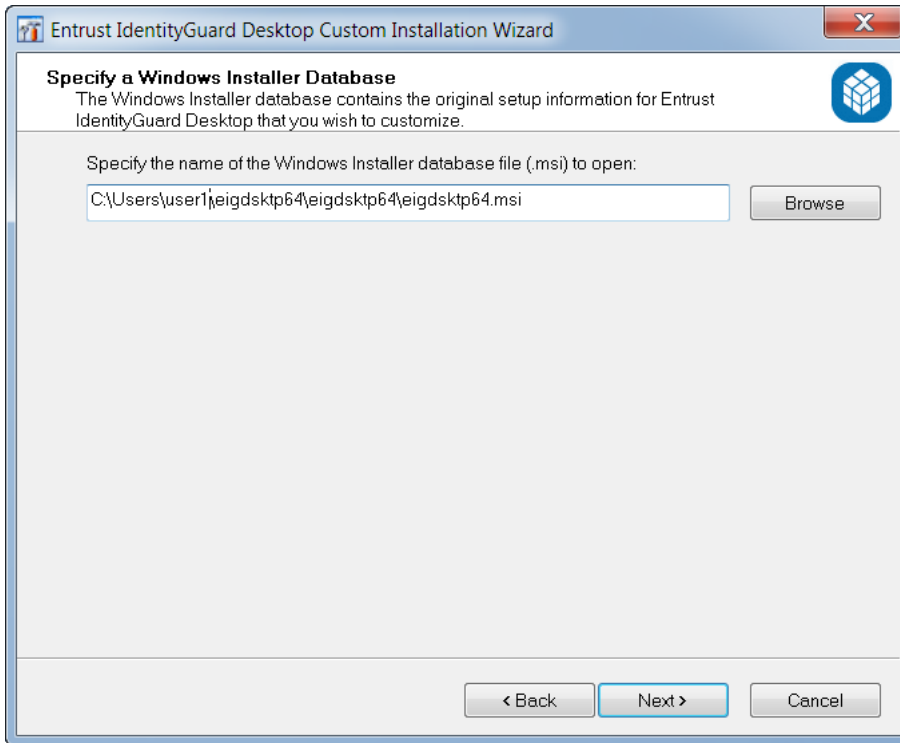
- a Navigate to the <IDG\_CP\_12.0\_extracted\_folder>\Utilities\ folder.
- b Double-click eigwincustwiz64.exe. (or eigwincustwiz32.exe).

The **Desktop Setup** wizard appears.



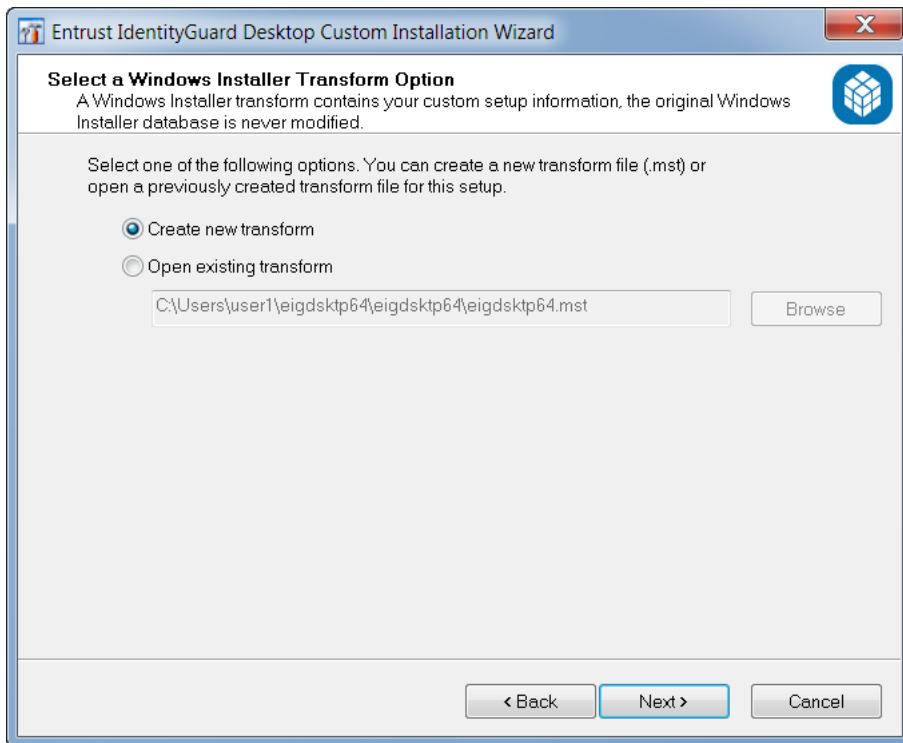
- 3 On the **Welcome** page, click **Next** to start customizing the installation.

The **Specify a Windows Installer Database** page appears.



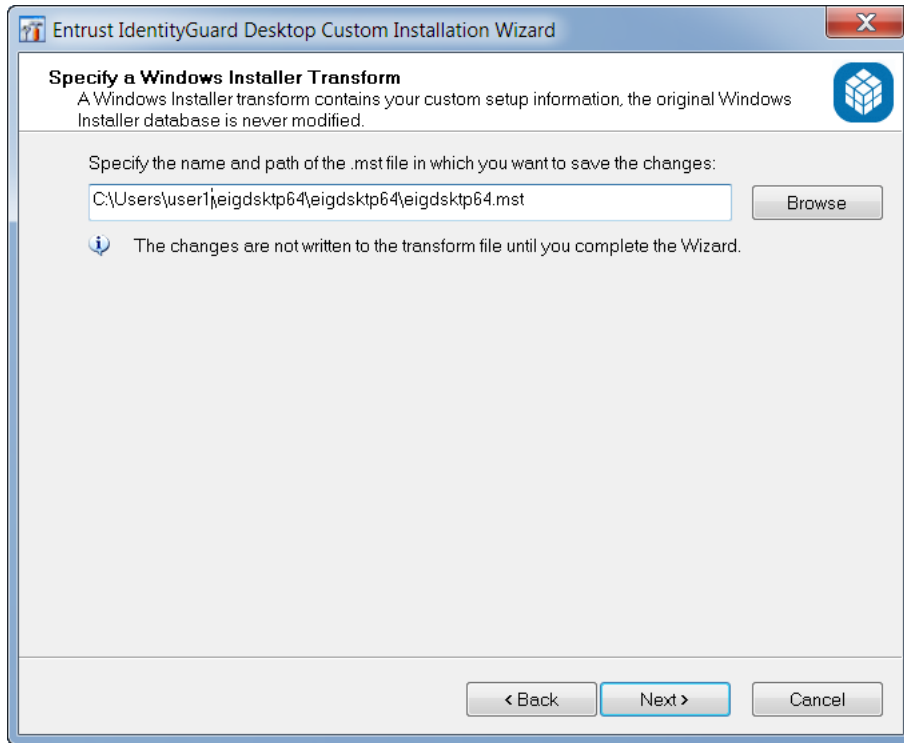
- 4** Enter the path for the Entrust IdentityGuard Desktop for Microsoft Windows installation file (`eidgsktp64.msi` or `eidgsktp32.msi`). This file is included with your Entrust IdentityGuard Desktop for Microsoft Windows software.
- 5** Click **Next**.

The **Select a Windows Installer Transform Option** page appears.



- 6 Select **Create a new transform** if you do not have an existing transform file. If you have an existing transform file, choose **Open existing transform**, and **Browse** to your MST file.
- 7 Click **Next**.

The **Specify a Windows Installer Transform** page appears.



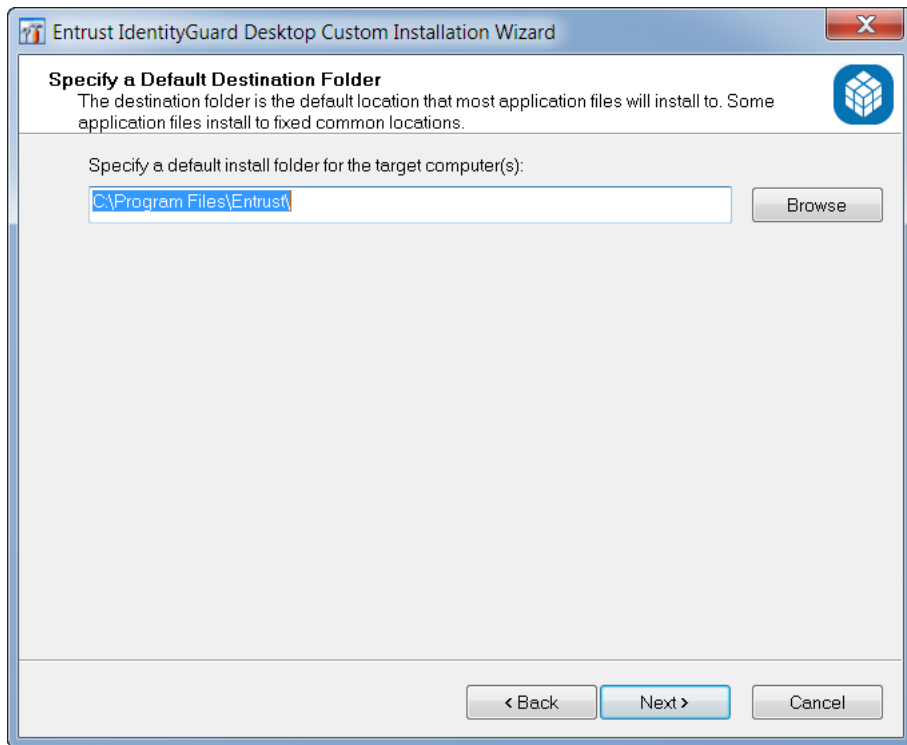
**Note:**

The transform file is not saved until the end of the wizard procedure. You can exit this wizard at any time before completing the transform file by clicking **Cancel**. To save the transform (MST) file before completing it, click **Next** until you reach the end of the wizard. You can save the transform (MST) file to return to it later for editing.

- 8 If you are creating a new transform file, specify the path and the file name. Browse to the MST file in which to save your custom setup information and click **Next**.

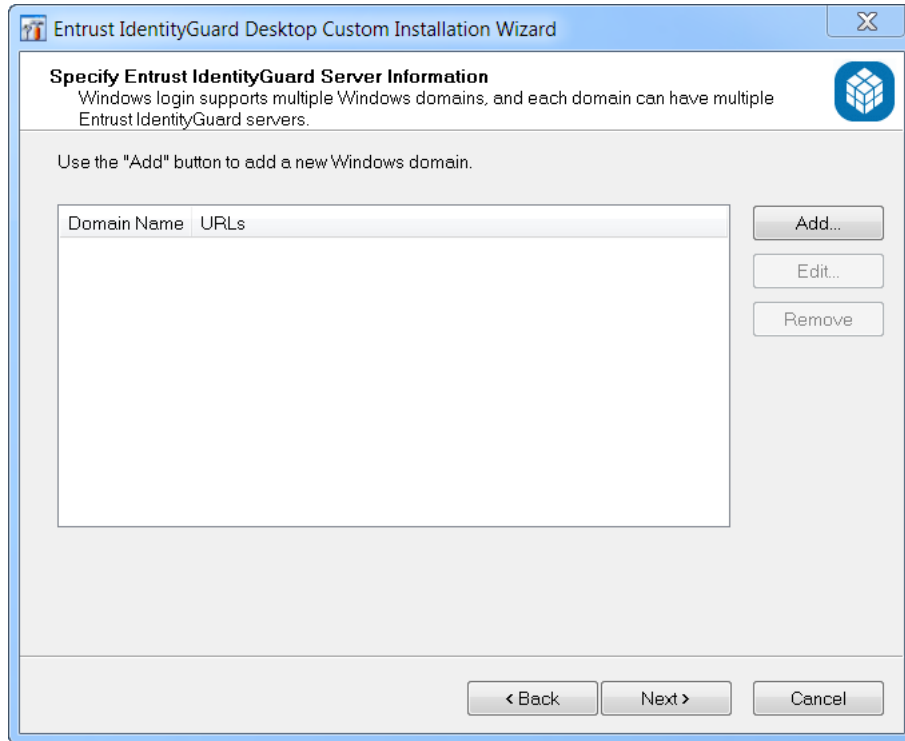


The **Specify a Default Destination Folder** page appears.



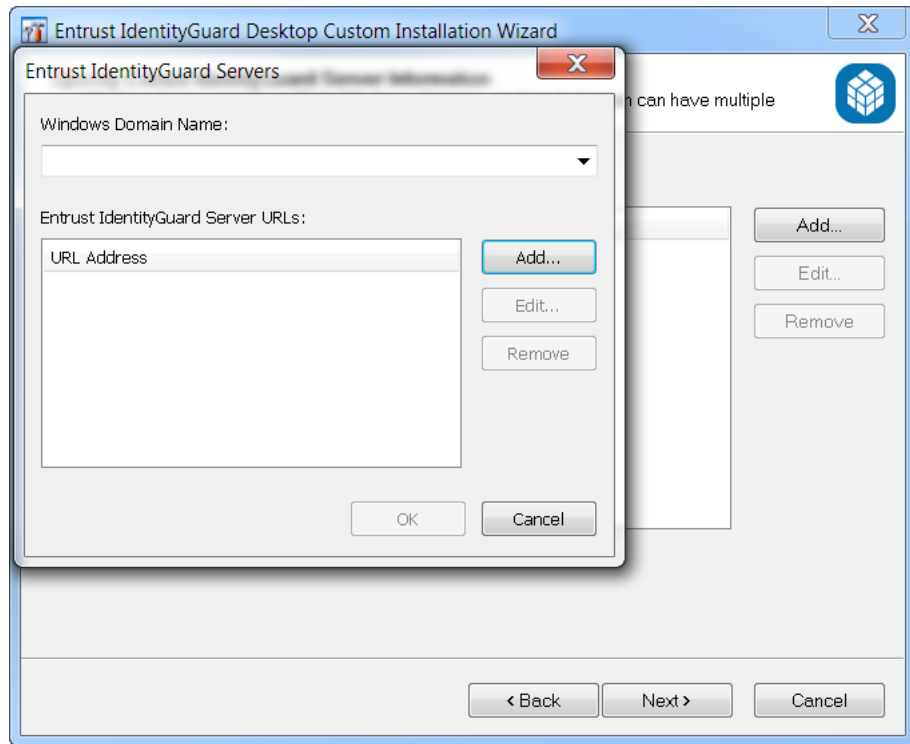
- 9 Select the default installation folder on the target computer and click **Next**.

The **Specify Entrust IdentityGuard Server Information** page appears.



**10** To add Windows domains and Entrust IdentityGuard Server URLs:

- a** Click **Add**.



- b** Under **Windows Domain Name**, enter the name of the domain where the client computer is located. This is the name of the domain in which the user's computer is located, not the domain where Entrust IdentityGuard Server is located.

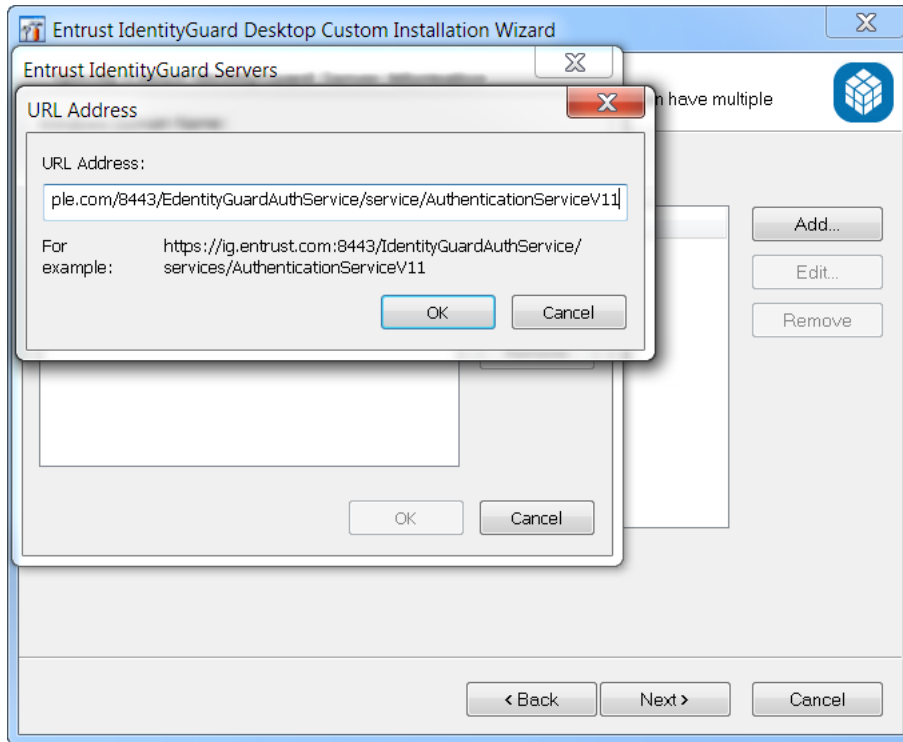


**Note:**

Domain names cannot contain spaces.

- c** On the Entrust IdentityGuard Servers dialog box, click **Add**.

The **URL Address** page appears.



- d** Enter the Entrust IdentityGuard Server HTTPS URL Address in the text box. Be sure to append V11 to the end of each URL. The URLs should be similar to the following:

`https://ig.example.com:8443/IdentityGuardAuthService/service  
s/AuthenticationServiceV11`



**Note:**

Be sure that the host name in the IdentityGuard server URL matches the common name in the IdentityGuard server certificate. If the names do not match, the Entrust IdentityGuard Desktop for Windows will not be able to communicate with the Entrust IdentityGuard Server.

**Attention:**

The URL is not validated during the install. Ensure that you have typed the URLs correctly before moving to the next step.

- e** Click **OK**.

If you have more than one Entrust IdentityGuard Server in your environment, repeat [Step 10 a](#) to [Step 10 c](#) to add URLs for those servers.

Entrust IdentityGuard Desktop Client allows you to add multiple Entrust IdentityGuard Server URLs for the purposes of failover. The URLs you enter in this step are stored sequentially in the registry, in the same order as they appear in the list. When the user attempts to connect to the first URL, if the server is not available, the failover mechanism tries to connect to the next URL in the sequence, and so on down the list.

- f** To add domains repeat steps [Step 10 a](#) to [Step 10 e](#).

- 11** Click **Next** on the **Entrust IdentityGuard Server Information** page.

The **Entrust IdentityGuard Self-Service Module information** page appears.

Entrust IdentityGuard Desktop Custom Installation Wizard

**Specify Entrust IdentityGuard Self-Service Module information**

Windows login supports multiple Windows domains, and each domain can have multiple Entrust IdentityGuard self-service instances configured.

Use the "Add" button to add a new Windows domain.

Domain Name	URLs
-------------	------

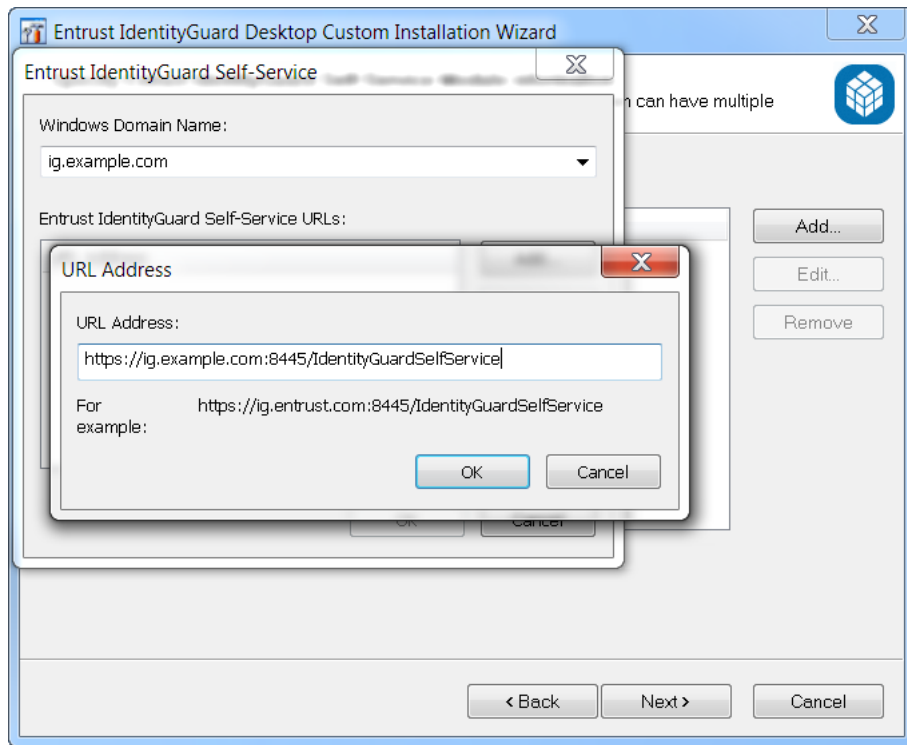
Add... Edit... Remove

< Back Next > Cancel

## 12 To specify Self-Service Server information:

- a Click **Add**.

The Entrust IdentityGuard Self-Service page appears.



- b From the **Windows Domain Name** drop-down list, select the domain for which you want to configure SSM.
- c To add the URL of the Self-Service Module, click **Add**, and then enter the URL of the Self-Service Module in the **URL Address** box.
- d Click **OK** to save the URL address.
- e Click **OK** to close the Entrust IdentityGuard Self-Service dialog box.

If you have more than one Entrust IdentityGuard Self-Service server in your environment, repeat [Step 12 a](#) to [Step 12 c](#) to add URLs for those servers.

Entrust IdentityGuard Desktop Client allows you to add multiple Entrust IdentityGuard Self-Service URLs. The URLs you enter in this step are stored sequentially in the registry, in the same order as they appear in the list. When the user attempts to connect to the first URL, if the server is not available, the failover mechanism tries to connect to the next URL in the sequence, and so on down the list.

- 13** Click **Next** on the **Entrust IdentityGuard Self-Service Module Information** page. The **Configure password-less and offline Token authentication options** page appears.

Entrust IdentityGuard Desktop Custom Installation Wizard

**Configure password-less and offline Token authentication options**  
Customize the behavior of Windows login and offline Token authentication

Options for Password-less Login

- ☒ Enable password-less authentication
- ☒ Store Active Directory password in IdentityGuard server

Options for Offline Token Authentication

Specify the token download time (in hours)

Options for Fallback Authentication

- ☐ Enable fallback authentication

Options for Combined Authentication

- ☐ Enable combined authentication

< Back   **Next >**   Cancel

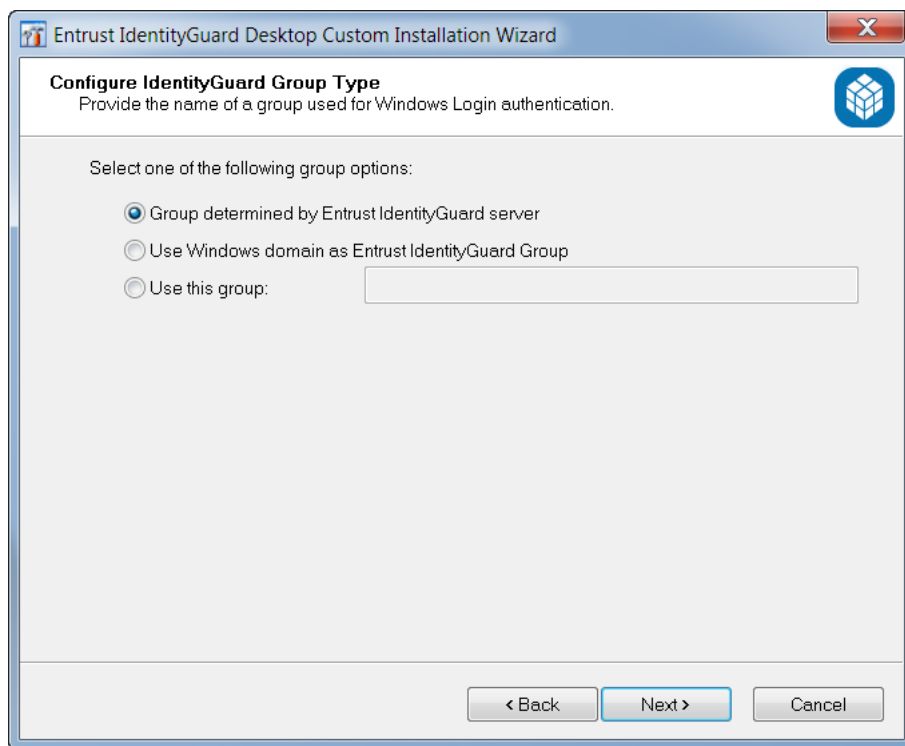
- 14** To specify the password-less, offline token, fallback authentication, and combined authentication options:
- a** Select **Enable password-less authentication** and **Store Active Directory password in IdentityGuard server** if you want to allow a user to be able to skip first factor authentication after initial log in.
  - b** To allow for **Offline token authentication**, enter a value in the **Specify the token download time (in hours)** to set the amount of time, in hours, that Entrust IdentityGuard Desktop for Windows allows offline token authentication. For more information on how offline token authentication works, see [“How the offline token works” on page 57](#).
  - c** Select **Enable fallback authentication** if you want to allow users to use an alternate authenticator if their primary authentication method is unavailable.
  - d** Select **Enable combined authentication** if you want first- and second-factor authentication challenges to be evaluated at the same time.

**Note:**

**Enable combined authentication** and **Enable password-less authentication** cannot be used at the same time. If both are checked, then Enable combined authentication will override Enable password-less authentication and EnablePwdless will be disabled.

**15 Click Next.**

The **Configure IdentityGuard Group Type** page appears.

**16 Configure how groups are to be handled.** If user names are unique in your Entrust IdentityGuard environment, the group can be determined by Entrust IdentityGuard Server.

If user names are not unique, use the Windows domain option or the name of the group that includes all users who will receive this package. If you are specifying a group or using a Windows domain, you must create and deploy separate packages for the users in each group or domain. For example, you



would create a package for all users in group A and a different package for all users in group B.

- To allow Entrust IdentityGuard to set the group, select **Group determined by Entrust IdentityGuard Server**.
- To use the Windows domain as the group, select Use Windows domain as **Entrust IdentityGuard Group**.
- To enter the group name to use, select **Use this group**, and enter the group name in the text box.

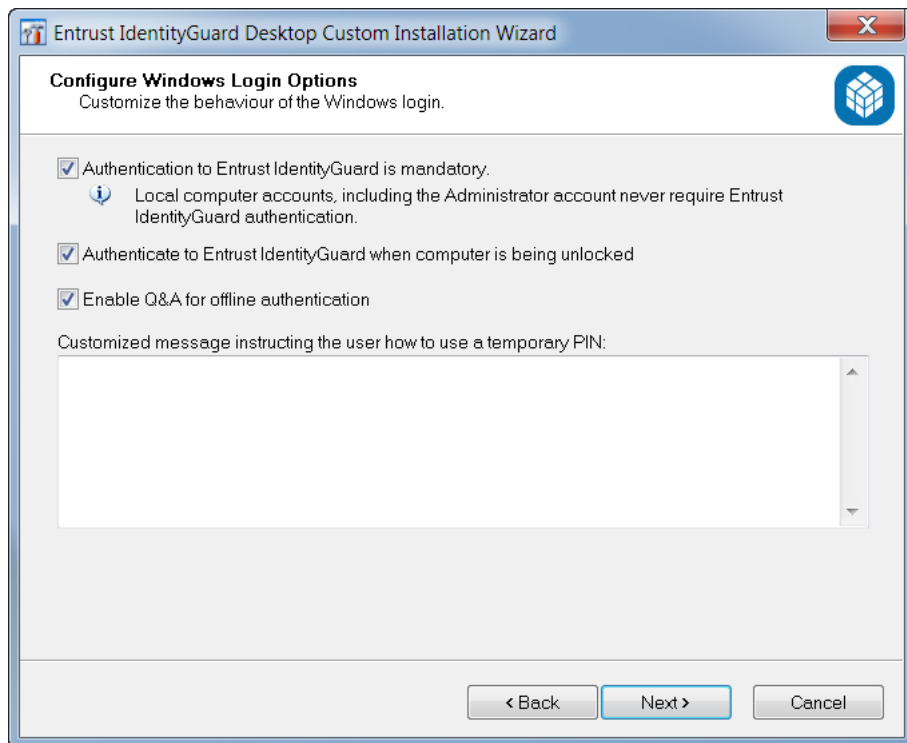


**Note:**

Group names cannot contain spaces.

**17** Click **Next**.

The **Configure Windows Login Options** page appears.



**18** To configure Windows login options:

- To require all users to authenticate to Entrust IdentityGuard, select **Authentication to Entrust IdentityGuard is mandatory**.



**Note:**

Local computer accounts, including the Administrator account, never require Entrust IdentityGuard authentication.

---

- To require users to authenticate when unlocking their computers, select **Authenticate to Entrust IdentityGuard when computer is being unlocked**. If you deselect this box, users that are not registered in Entrust IdentityGuard will be able to log in without a second factor challenge.
- To enable users to log in to the computer offline using question and answer authentication, **Select Enable Q&A for offline authentication**.
- To set a customized information message to tell your users how to use a temporary PIN, enter your text in **Customized message instructing the user how to use a temporary PIN**.



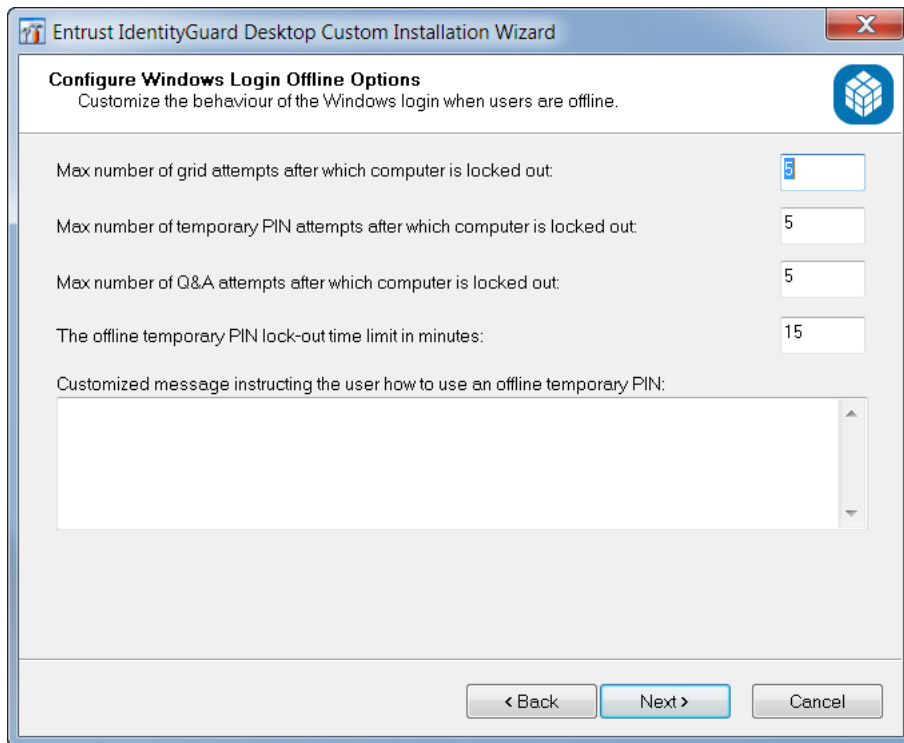
**Note:**

Add custom text here if your users need special instructions or instructions in another language.

---

**19** Click **Next**.

The **Configure Windows Offline Options** page appears.



Entrust IdentityGuard Desktop Custom Installation Wizard

**Configure Windows Login Offline Options**  
Customize the behaviour of the Windows login when users are offline.

Max number of grid attempts after which computer is locked out: 5

Max number of temporary PIN attempts after which computer is locked out: 5

Max number of Q&A attempts after which computer is locked out: 5

The offline temporary PIN lock-out time limit in minutes: 15

Customized message instructing the user how to use an offline temporary PIN:

< Back Next > Cancel



**Note:**

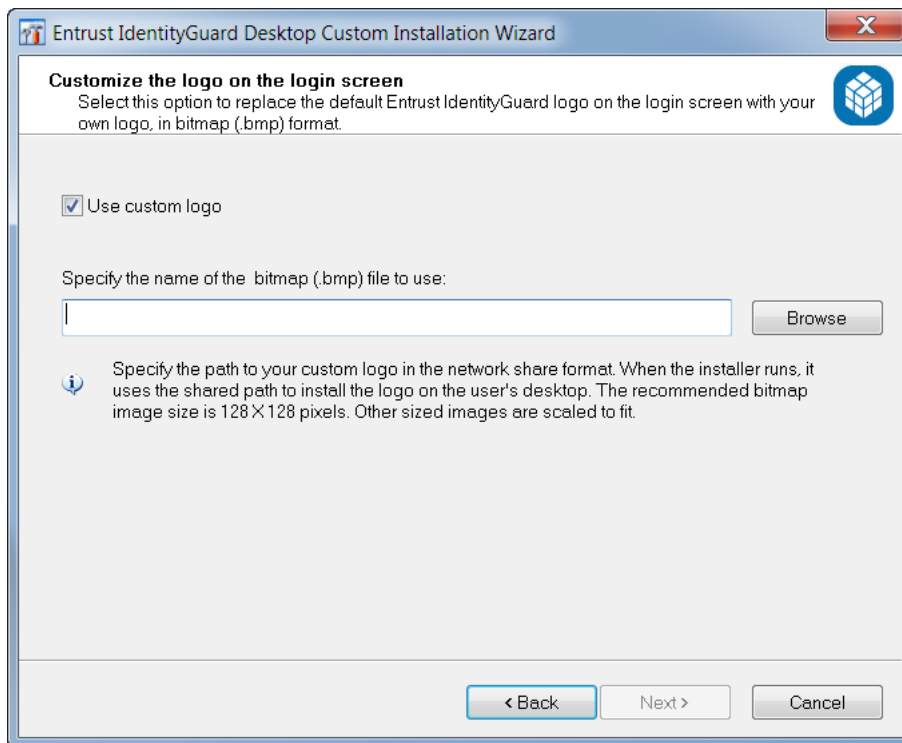
Add custom messages if your users need special instructions, or instructions in another language.

**20** On the **Configure Windows Login Offline Options** page:

- Enter a value in **Max number of challenge attempts after which computer is locked out**. The default is 5 and the maximum is 1000.
- Enter a value in **Max number of temporary PIN attempts after which the computer is locked out**. The default is 5.
- Enter a value in **Max number of Q&A attempts after which the computer is locked out** for the maximum number of Q&A attempts. The default value is 5.
- Enter a value in **The offline temporary PIN lock-out time limit in minutes**. The default is 15. The lockout time value must be between 1 and 14400.
- In the **Customized message instructing the user how to use an offline temporary PIN** text box, enter instructions telling users how to use an offline temporary PIN.

**21** Click **Next**.

The **Customize the logo on the login screen** page appears.



- 22** If you want to replace the default Entrust IdentityGuard logo with your organization's logo on the desktop login screen, select **Use Custom Logo**, and then click **Browse** to navigate to the location of the image file.

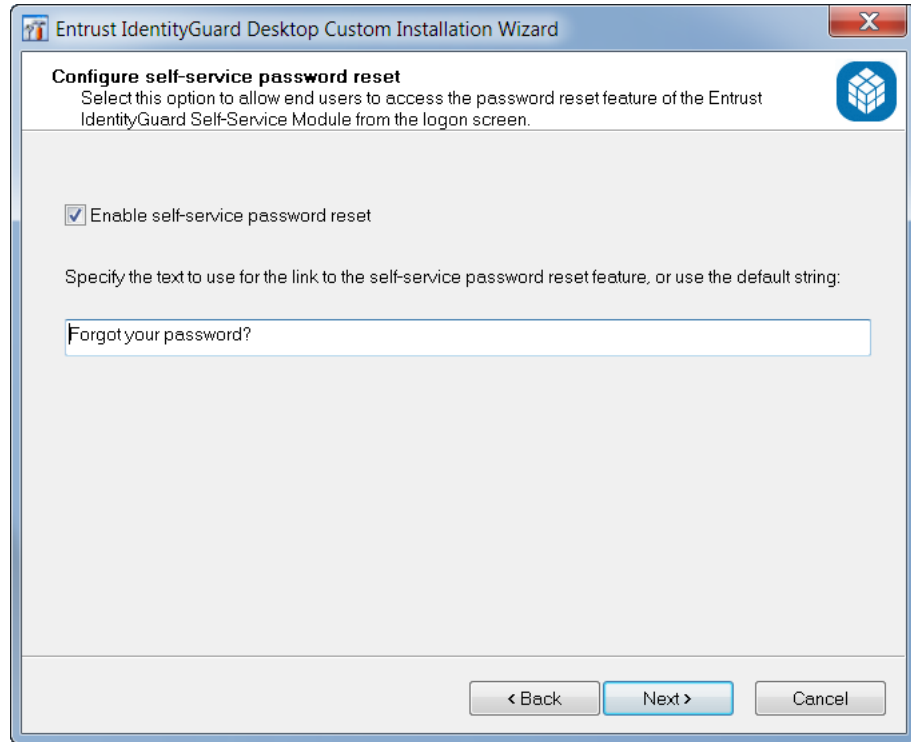
The image must be located in a network share accessible to users when they install the desktop client. The path must be in the following format:

\\<path>\<image\_file>.bmp

The logo image must be in bitmap form (.bmp). The recommended size of the image is 128 X 128 pixels. If the image is smaller or larger, it will be scaled to fit the available space.

**23** Click **Next**.

The **Configure self-service password reset** page appears.



- 24** If you want users to be able to access the Entrust IdentityGuard Self-Service Module (SSM) to reset forgotten passwords, select **Enable self-service password reset**. When this option is selected, a link to SSM appears on each user's login page.



**Note:**

For important information on using this feature, see [“IdentityGuard Desktop client integration with SSM” on page 161](#).

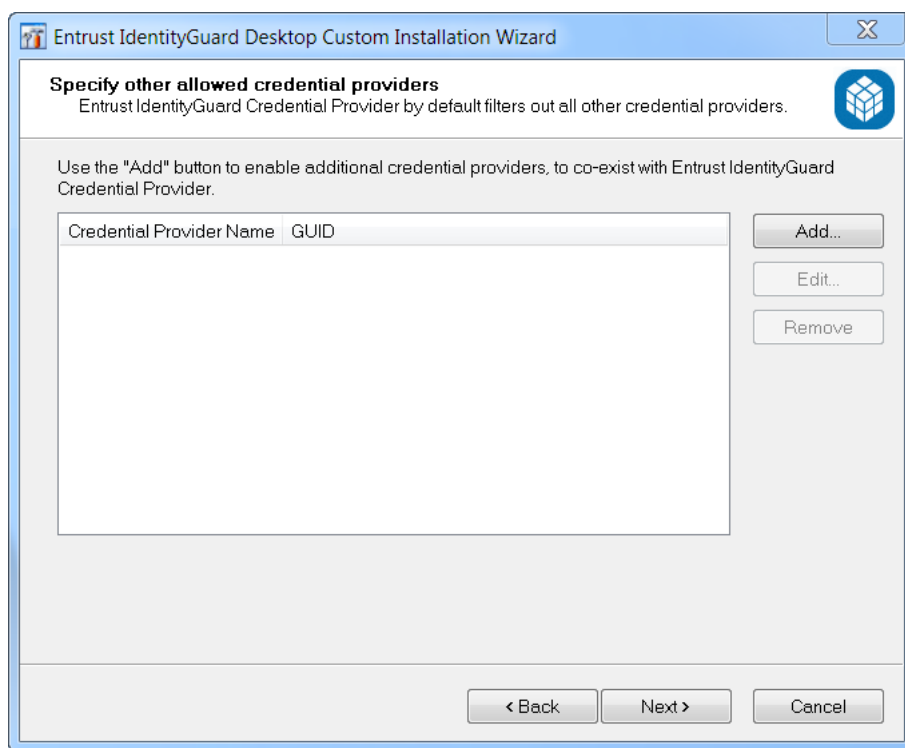
**Note:**

If you enable this feature, in addition to the settings you configure in this wizard, the password reset feature must be enabled in SSM (see [“Configuring the Self-Service Module settings for password reset” on page 75](#)).

**25** If you want to customize the text of the link the SSM, enter a new text in the text box. Otherwise, the default text is used.

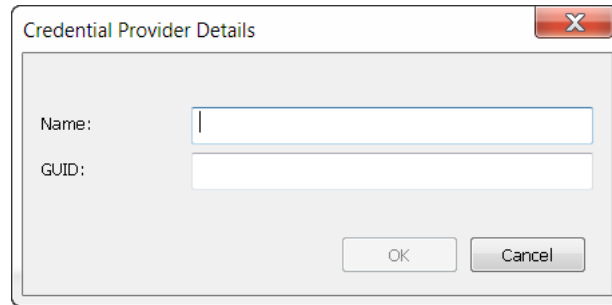
**26** Click **Next**.

The **Specify other allowed credential providers** page appears.



**27** You can use this wizard to add other credential providers to Entrust IdentityGuard Desktop, or you can add them from a `AllowCredentialProviders.ini` file, as described in [“Adding certification providers from a file” on page 142](#). If you have already added other credential providers using the `AllowCredentialProviders.ini` file, the other credential providers appear in the list. If you want to add a credential provider, click **Add**.

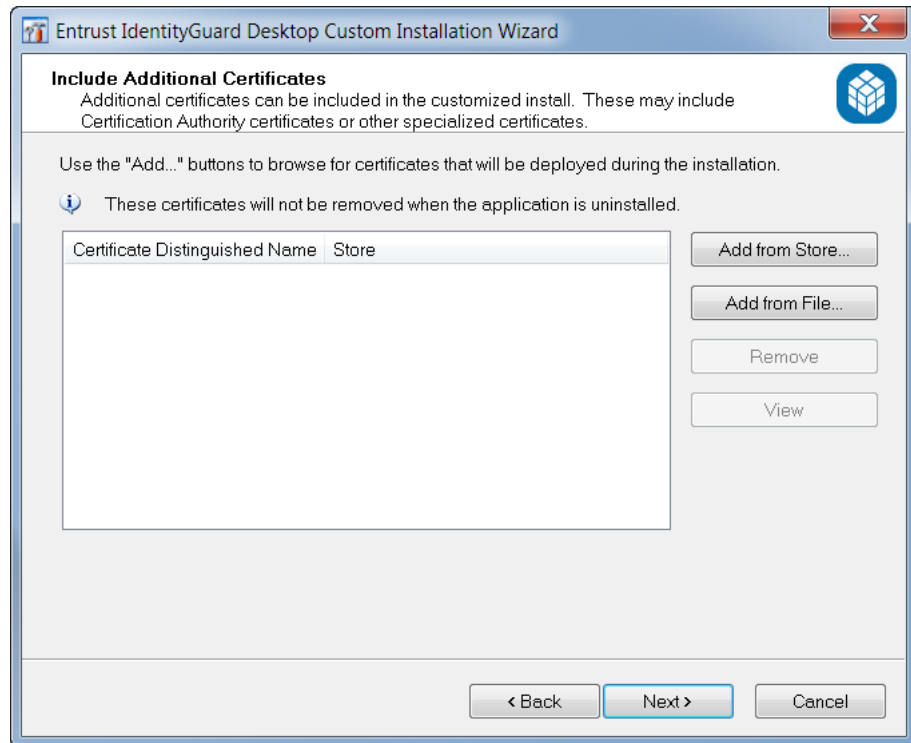
The Credential Providers Details dialog box appears.test



The dialog box is titled "Credential Provider Details" and has a close button (X) in the top right corner. It contains two text input fields: "Name:" and "GUID:". Below these fields are two buttons: "OK" and "Cancel".

- 28** Enter the name of the credential provider and the globally unique identifier (GUID) for the credential provider, and then click **OK**.

The **Include Additional Certificates** page appears.



The page is titled "Include Additional Certificates" and is part of the "Entrust IdentityGuard Desktop Custom Installation Wizard". It contains the following text: "Additional certificates can be included in the customized install. These may include Certification Authority certificates or other specialized certificates." and "Use the 'Add...' buttons to browse for certificates that will be deployed during the installation." Below this text is an information icon (i) and the text: "These certificates will not be removed when the application is uninstalled." There is a table with two columns: "Certificate Distinguished Name" and "Store". To the right of the table are four buttons: "Add from Store...", "Add from File...", "Remove", and "View". At the bottom of the page are three buttons: "< Back", "Next >", and "Cancel".

- 29** Add the certificates that will be deployed during installation, as follows:

- If installing for **Entrust IdentityGuard** add the certificate from the Entrust IdentityGuard Server described in the section "[Communication between](#)

Desktop for Microsoft Windows and the Entrust IdentityGuard Server" and any other certificates that may be required for secure communication.

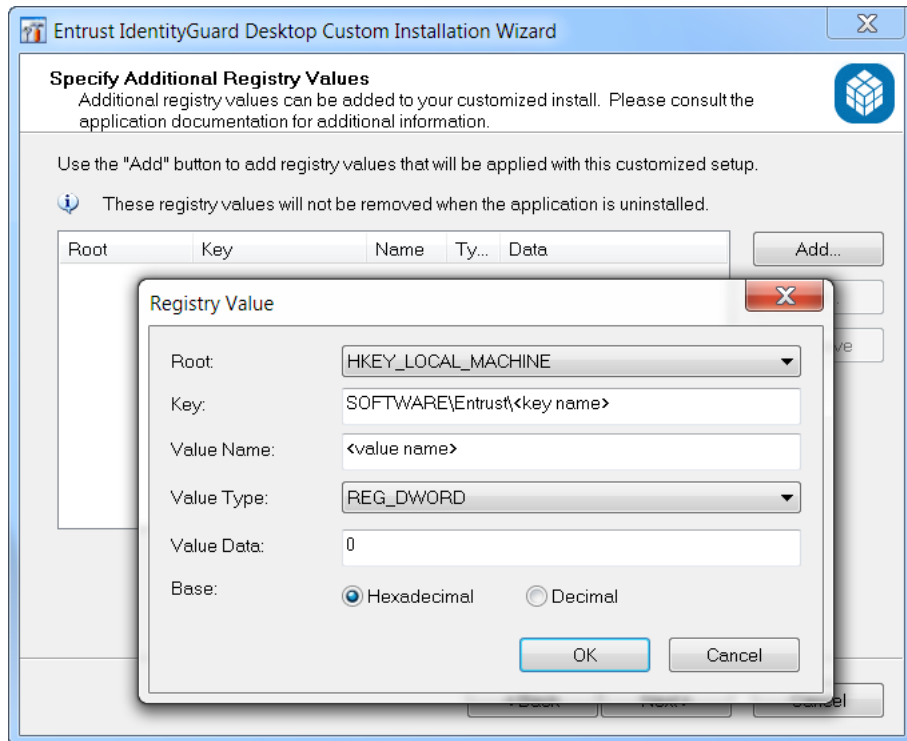
- If installing for **IntelliTrust**, add the certificate that you downloaded from the Gateway instance. See the section on "Integrating Entrust IdentityGuard Desktop for Windows" in the *IntelliTrust Online Help* for more information.

To add the certificate, click either:

- **Add from Store**
  - The **Select Certificate** dialog box appears. Select the certificates and click **OK**.
- **Add from File**
  - The **Browse For Certificate** dialog box appears. Browse for the certificate, then click **Open**.

**30** Click **Next**.

The **Specify Additional Registry Values** page appears.



- 31** Registry values are used to configure the package to your needs. Some values have already been specified by your choices in previous pages in the wizard. Click **Add** to add configuration choices to the installation package (see "[Registry settings](#)" on page 145).



**Note:**

If you selected the **Enable self-service password reset** option in [Step 24](#), see more information in ["IdentityGuard Desktop client integration with SSM" on page 161](#).

---

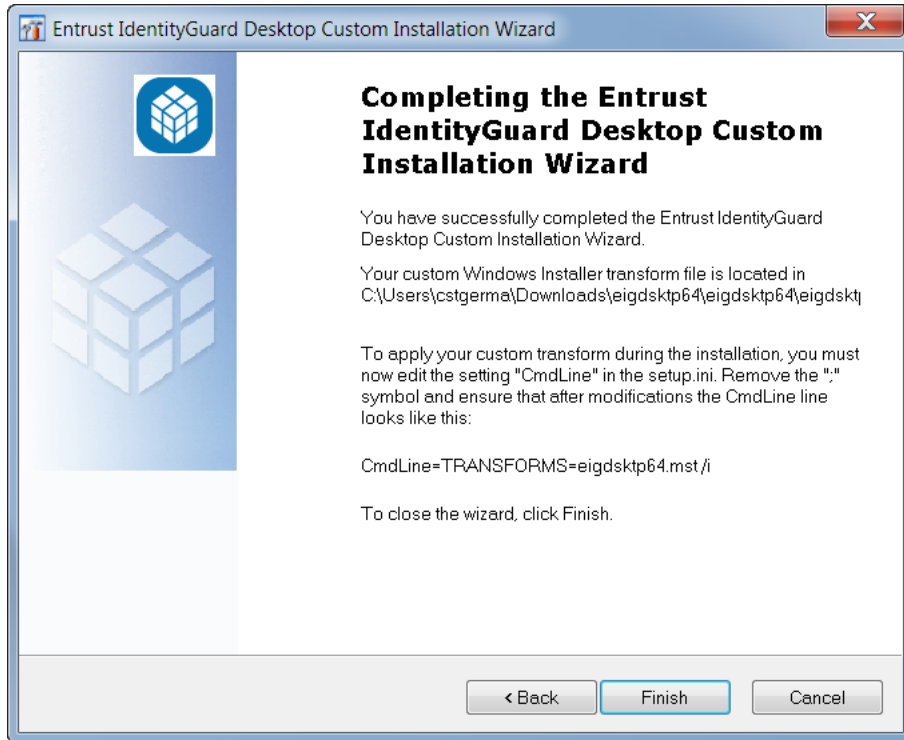
- a** To add a registry value, in the **Registry Value** dialog box, select a root computer from the **Root** drop-down list, and enter the **Key**, **Value Name**, **Value Type** and **Value Data**.
- b** After you have entered all your settings, click **OK**.
- c** To add another registry value, click **Add** and repeat steps a and b.
- d** After you are finished adding registry values, click **Next**.

**Attention:**

The installation does not automatically enable the `ProhibitFallbacks` registry setting during installation. This setting is used to force users to enter second-factor authentication when logging on in Windows Safe Mode. If users log in to the computer in Safe Mode, they are not required to use second-factor authentication. For information about the benefits and drawbacks of enabling this setting, see ["ProhibitFallbacks" on page 160](#).

---

The **Completing the Entrust IdentityGuard Desktop Custom Installation Wizard** page appears.



- 32** Read the instructions for applying the custom transform file (MST) during the installation. See [“Applying your custom transform file during installation” on page 107](#) for further instructions.
- 33** Click **Finish** to close the wizard and save the transform file.

## Installing biometric drivers

After installing Entrust IdentityGuard Desktop for Windows, you need to manually install the biometric drivers.

### To manually install biometric drivers

- 1** Open a command prompt window.
- 2** Go to `C:\Program Files\Entrust\IdentityGuard Fingerprint Enrollment Client\driver\` and run the following:
  - **DPInst.exe** for 32-bit
  - **DPInst64.exe** for 64-bit

## Applying your custom transform file during installation

When you finish creating your custom transform (MST) file using the **Entrust IdentityGuard Desktop Custom Installation** wizard, edit the `setup.ini` file to apply your custom transform file during installation.

### To apply your custom transform file during installation

- 1 Open the `setup.ini` file in a text editor. The `setup.ini` is part of the Entrust IdentityGuard Desktop for Microsoft Windows software.
- 2 The following information is located at the end of the `[Wise Installer]` section of the `setup.ini` file:

```
;To apply a transform, please remove the ";" symbol in the  
following line and replace "eigdsctp64.mst" with the name of the  
transform you want to apply.
```

```
;CmdLine=TRANSFORMS=eigdsctp64.mst /i
```

- 3 Remove the semicolon (;) at the beginning of the line beginning with `CmdLine`. Replace the default MST file name with the file name you choose for your custom transform. For example, if you choose the file name `eigdsctp64.mst`, the `setup.ini` will look like this:

```
;To apply a transform, please remove the ";" symbol in the  
following line and replace "eigdsctp64.mst" with the name of the  
transform you want to apply.
```

```
CmdLine=TRANSFORMS=eigdsctp64.mst /i
```

- 4 Save and close the file.

## Testing the installation package

After creating the installation package, test it by running it in a test environment.

# Providing the installation package as an executable or as a Windows Installer file

The `setup.exe` file launches the Entrust IdentityGuard Desktop for Microsoft Windows Installer package (`eigdsktp64.msi` or `eigdsktp32.msi`) and the installation begins.

---

**Note:**

If you want users to install the software by running the `setup.exe`, you must also copy the `eigdsktp64.msi` (or `eigdsktp32.msi`) file to the same location as the `setup.exe` file. If you have also created a transform (MST) file to apply to your custom installation package, ensure that the `setup.ini` file reflects that location.

---

See [“Distributing the installation package” on page 109](#) for further information about making the installation files available to users.

# Distributing the installation package

By running the **Custom Installation** wizard (`eigwincustwiz64.exe` or `eigwincustwiz32.exe`), you have created a Microsoft Windows Installer transform file (MST). When you finish creating the custom installation package using the transform file, you can distribute the software to users for installation.

If you are making the installation package available from a network location, you can run the custom setup in Administrative mode to extract the Windows Installer file and Entrust IdentityGuard Desktop for Microsoft Windows application files to a specified location.

After you distribute the Custom Installation package to your users, they can run the setup file (`setup.exe`).

This section describes the available distribution and installation options:

- [“Making the installation package available on the network” on page 109](#)
- [“Making the installation package available on the Web” on page 110](#)
- [“Using third-party software distribution tools” on page 111](#)
- [“Performing a silent installation” on page 111](#)

## Making the installation package available on the network

You can run the Windows Installer file (`eigdsktp64.msi` or `eigdsktp32.msi`) or the setup executable file (`setup.exe`) in administrative mode. This enables you to specify a network location to which to post the Windows Installer package so that you can make it available to users over your local network. Using administrative mode extracts the Windows Installer file (`eigdsktp64.msi` or `eigdsktp32.msi`), which contains Entrust IdentityGuard Desktop for Microsoft Windows application files, to the specified location.



### Note:

You must have the appropriate file permissions to successfully complete the extraction.

---

- 1 Enter the following command to run the `setup.exe` from a command prompt, or from the **Run** command of the **Start** menu. Execute the following command:

```
[<full path> setup.exe] /a
```

where:

- `<full path>` is the full path to the EXE file
- `/a` runs installation in Administrative mode

**2** Enter the network installation point at the prompt, and the extraction will begin. The Entrust IdentityGuard Desktop for Microsoft Windows files are extracted into a folder structure that represents the destination folders for the files installed on the user system.

There are various methods available to enable users to easily install custom installation packages from the network. Use your organization's usual distribution method. Some methods are:

- Create a batch file that runs the Windows Installer file along with the appropriate transform file, and distribute the batch file to users.
- Create a shortcut for the transform file, and have users run the shortcut.
- Add a transform to the executable provided with Entrust IdentityGuard Desktop for Microsoft Windows (`setup.exe`) to run both the Windows Installer file and applicable transform file. See ["To apply your custom transform file during installation" on page 107](#) for complete instructions.

You can also use third-party software distribution tools to manage and distribute software to users. See ["Using third-party software distribution tools" on page 111](#) for further information.

## Making the installation package available on the Web

When making the installation package available on the Web, you must ensure that your users have the Windows Installer Service available on their computers.

If the installation database is at a URL, the installer downloads the database to a cache before starting the installation.

Windows Installer also downloads the appropriate files to complete the installation for the user's selections. For example, to install a package with a source located on a Web server at `http://<path_to_files>/eigdsctp64.msi` (or `eigdsctp32.msi`), use the following instructions:

- 1** Include a link to a batch file on the a Web page, for example, `setup.bat`.
- 2** Enter the following command in the batch file:

```
msiexec /i http://<path_to_files>/eigdsctp64.msi  
TRANSFORMS=http://<path_to_files>/eigdsctp64.mst
```

When the user clicks `setup.bat` in the browser, the installation begins.



### Note:

Do not instruct users to install the installation package using the MSI file directly, rather than the `setup` file, if the MSI file requires other supporting files for the installation.

---

## Using third-party software distribution tools

Various third-party desktop software management and distribution tools can be used to enable easy deployment and management of software to organizations.



### Note:

Entrust does not make any recommendations about which tool to use.

---

Two examples of suitable third-party software distribution tools are:

- Microsoft® Systems Management Server. See <http://www.microsoft.com>.
- The IBM® Tivoli product portfolio. See <http://www.tivoli.com>.

## Performing a silent installation

If you want to provide an installation package that requires a minimum of input from users as it runs, you can set up your installation package for silent installation.

When implementing a silent installation, you can configure how much interaction users have with the installation by including a command line parameter in the `setup.ini` file. When the setup executable file (`setup.exe`) runs, the command line parameter is executed.

After creating your custom transform (MST) by completing the **Custom Installation** wizard, edit the `setup.ini` file to apply the custom transform to all users instead of the current user during installation.

### To perform a silent installation for all users

- 1 Open the `setup.ini` file in a text editor. The following information is located at the end of the `[WiseInstaller]` section:

```
;To apply a transform, please remove the ";" symbol in the  
following line and replace "eigdsctp64.mst" with the name of the  
transform you want to apply.
```

```
;CmdLine=TRANSFORMS=eigdsctp64.mst /i
```

- 2 Remove the semicolon (;), and replace

```
CmdLine=TRANSFORMS=eigdsctp64.mst /i
```

with

```
CmdLine=ALLUSERS=1 /q TRANSFORMS=<path to your .mst>
```

# Modifying silent installation options

Choose one of the command line options in [Table 3 on page 112](#) to add to your `setup.ini` file, depending on your requirements.

For example:

```
CmdLine=/qn+
```

**Table 3:** Silent installation command line parameters

CmdLine=	Parameters
/q or /qn	No user interface (UI) displayed to user during installation.
/qn+	No UI displayed, except for a modal dialog box displayed at the end of the installation.
/qb	Basic UI displayed.
/qb!	Basic UI that hides the <b>Cancel</b> button.
/qb+	Basic UI with a modal dialog box displayed at the end of the installation. The modal dialog box is displayed if the user cancels the installation.
/qb+!	Basic UI, hiding the <b>Cancel</b> button, with a modal dialog box displayed at the end of the installation.
/qb-	Basic UI, with no modal dialog boxes.
/qb-!	Basic UI, hiding the <b>Cancel</b> button, with no modal dialog boxes.
/qr	Reduced UI with no modal dialog box displayed at the end of the installation.
/qf	Full UI and any authored <b>Fatal Error</b> , <b>User Exit</b> , or <b>Exit</b> modal dialog boxes at the end of the installation.



# Creating an administrative installation

Typically, administrators deploy Entrust IdentityGuard Desktop for Microsoft Windows by distributing a package to users containing a `setup.ini`, `setup.exe`, `<filename>.mst`, and `<filename>.msi` file. An alternative to this distribution mechanism is the administrative installation.

Using an administrative installation, the administrator creates an installation package and makes it available to end users from a central location. The software is deployed to end users using various distribution strategies. System administrators can investigate distribution options by visiting the Microsoft Web site. The following links lead to documents that discuss how to configure an administrative installation:

- [http://msdn2.microsoft.com/en-us/library/aa367541\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa367541(VS.85).aspx)
- <http://technet.microsoft.com/en-us/library/bb742606.aspx>

After you apply a patch or service pack to an existing administrative installation, you must redistribute the updated MSI file to the end users. There are several methods available for performing the update.

This section contains examples of how to set up an administrative installation that uses a batch file. If you prefer to use another strategy, and require assistance, consult the documentation on the Microsoft Web site.

**Note:**

Procedures in this section use the filenames for the 64-bit version of the software, however, they apply to the 32-bit version as well.

---

## Fresh installation: no existing Entrust IdentityGuard Desktop for Microsoft Windows software on users' computers

This procedure describes how to create an administrative installation if a new software installation is required (the desktop does not have a prior installation of Entrust IdentityGuard Desktop for Microsoft Windows).

## Assumptions

The following is assumed when using this procedure:

- This procedure is being used with a fresh installation that does not include an Entrust IdentityGuard Desktop for Microsoft Windows patch.
- This procedure uses a batch file to install the software. For information about other options, consult the Microsoft Web site.
- The installation is intended to start when the Entrust IdentityGuard Desktop for Microsoft Windows end user double-clicks the BAT file on their desktop.

## Administrative installation package contents

The Administrative install package contains the following files:

- BAT (this is distributed to users—all other files must be placed in a centralized location like a URL or UNC path)
- application files
- MSI (this is the base installer)
- MST (this contains your installer customization)

### To create an administrative installation package

**1** From a command line, change to the directory containing your MSI file.

**2** Run an administrative installation by typing the following command:

```
msiexec /a <msifilename>.msi
```

where <msifilename> is the name of your MSI file.

For example, `c:\eigdsktp64.msi`

The **Admin Installation** dialog box appears.

**3** Under **Network installation point**, specify a network folder in which to place the Administrative Install.

**4** Click **Next**.

The **Admin Installation Verify Ready** dialog box appears.

**5** Click **Next**.

The installer extracts the application files from the MSI file and places them in folders at the network location you specified.

You now have an administrative installation that you can distribute.

**6** Copy your MST files to the administrative installation directory.

**7** Create a BAT file that users can double-click to install Entrust IdentityGuard Desktop for Microsoft Windows. The BAT file contains a command to run a specified MST file against the MSI file. To create a BAT file:

- a** Open a text editor such as Notepad.
- b** Type the following:

```
msiexec /i <filepath>.msi TRANSFORMS=<filepath>.mst
```

where <filepath> is replaced with the full path and name of your MSI and MST files. The path can be a UNC path or a URL path.

Example of a UNC path:

```
msiexec /i "\\nwksvr\IG\eigdsctp64.msi" TRANSFORMS="\\nwksvr\IG\eigdsctp64.mst"
```

Example of a URL path:

```
msiexec /i "http://svr/eigdsctp64.msi" TRANSFORMS="http://svr/eigdsctp64.mst"
```



**Note:**

Relative paths are not acceptable.

---

- c** If you want the installation to run silently—that is, without requiring user input—add /q to the command.

```
msiexec /i <filepath>.msi TRANSFORMS=<filepath>.mst /q
```

The /q parameter is one of several available parameters. Enter `msiexec` at the command prompt to display a full list of available parameters.

- 8** Repeat [Step 7](#) for each MST file in your deployment.

You now have a single Administrative install as well as one BAT file for each MST file.

After you test the installer, you can distribute the BAT file to users through email or another means. The user double-clicks the batch file to start the installation.

## Adding a patch or service pack to an existing installation

This procedure demonstrates how use an administrative installation with a patch or service pack.

## Assumptions

The following is assumed when using this procedure:

- This procedure is being used to add a service pack or patch to existing software.
- This procedure uses the simplest case scenario—for example, although the service pack or patch file (MSP) can be referenced from another folder, it is placed in the same folder as the MSI file in [Step 1 on page 117](#).
- This procedure uses a batch file to start and control the installation. For information about other options consult the Microsoft Web site.
- The installation is intended to start when the Entrust IdentityGuard Desktop for Microsoft Windows user double-clicks the BAT file on their desktop.

## Administrative install package contents

The Administrative install package contains the following files:

- BAT (this is distributed to users; all other files must be placed in a centralized location like a URL or UNC path)
- application files
- MSI (this is the base installer)
- MST (this contains your installer customization)
- MSP (this is a patch or service pack)

### To create an administrative package (patch or service pack)

- 1 Ensure that your patch or service pack file (MSP) is in the same directory as your MSI file.
- 2 From a command line, change to the directory containing your MSI file.
- 3 Run an Administrative install by entering the following command:

```
msiexec /a <msifilename>.msi /p <mspfilename>.msp
```

where <msifilename> is the name of your MSI file and <mspfilename> is the name of a patch or service pack.

The **Admin Installation** dialog box appears.

- 4 Under **Network installation point**, specify a network folder in which to place the Administrative Install and then click **Next**.

The **Admin Installation Verify Ready** dialog box appears.

- 5 Click **Next**.

The application files are extracted from the MSI file and placed in folders at the network location you specified. Your installer (MSI) is updated with the latest patch or service pack contained in the MSP file.



#### Note:

To apply multiple patches or services packs, repeat [steps 3 to 5](#) for each MSP file. Entrust updates are normally cumulative so this should not be necessary. Check the instructions in the *Readme* file accompanying the patch.

You now have an administrative installation that you can package.

- 6 Create a BAT file that users can double-click to install Entrust IdentityGuard Desktop for Microsoft Windows. To create a BAT file:
  - a Open a text editor such as Notepad.
  - b Type the following:

```
msiexec /i <filepath>.msi REINSTALL=ALL REINSTALLMODE=vomus
```

where <filepath> is replaced with the full path and name of your MSI and MST files. The path can be a UNC path or a URL path.

Example of a UNC path:

```
msiexec /i "\\nwksvr\IG\eigdsctp64.msi" REINSTALL=ALL REINSTALLMODE=vomus
```

Example of a URL path:

```
msiexec /i "http://svr/eigdsctp64.msi" REINSTALL=ALL REINSTALLMODE=vomus
```



**Note:**

Do not use relative paths.

---

The reinstall command updates the Entrust IdentityGuard Desktop for Microsoft Windows software and the cached copy of the MSI on the end user system.

- If you want the installation to run silently—that is, without requiring user input—add /q.

```
msiexec /i <filepath>.msi REINSTALL=ALL REINSTALLMODE=vomus /q
```

The /q parameter is one of several available parameters. Type `msiexec` at the command prompt to display a full list of available parameters.

After you test the installer, you can distribute the BAT file to users through email or another means. The user double-clicks the batch file to start the installation.

# Saving the offline registry key when upgrading

When using the Windows Login feature in offline mode, the Entrust IdentityGuard Desktop for Microsoft Windows software creates numerous Windows registry settings for the offline use of the application. These settings are stored under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\OFFLINE
```

Uninstalling Entrust IdentityGuard Desktop for Microsoft Windows removes all registry settings under the OFFLINE key. However, you can remove the software and keep the OFFLINE key with the registry settings intact.

Keeping the OFFLINE key gives the user, who upgrades the software in the future in offline mode, the ability to log in to Entrust IdentityGuard Desktop for Microsoft Windows in offline mode without first logging in online.

## To save the offline registry key when upgrading

Instead of using the Control Panel feature **Programs and Features** (or **Add or Remove Programs**) or double-clicking the MSI to remove the software using one of the following procedures.

### Method 1

- 1 Using a text editor, create and run a batch file (.bat) that contains the following two lines (as appropriate for your installation):

```
msiexec.exe /x <product key> REMOVEWIGLOFFLINEKEY=0 /qn
```

```
msiexec.exe /i <MSI file> TRANSFORMS=<MST file>/qn
```

<MSI file> is the path to the customized Windows installer file

<MST file> is the path to the transform file



### Note:

To find the product key, open setup.ini and then copy the ProductCode in Notepad. For example,  
ProductCode={A123456F-4C812-7899-BA3E-01AA12345678}

---

### Example for a 64-bit installation:

```
msiexec.exe /x {A701206F-4F85-4581-BA3E-06FF750417A9} REMOVEWIGLOFFLINEKEY=0 /qn
```

```
msiexec.exe /i eigdsktp64.msi TRANSFORMS=eigdsktp64.mst /qn
```

### Example for a 32-bit installation:

```
msiexec.exe /x {4901F191-8957-47E2-B63A-7C8DE1D40C48} REMOVEWIGLOFFLINEKEY=0 /qn
```

```
msiexec.exe /i eigdsktp32.msi TRANSFORMS=eigdsktp32.mst /qn
```

The first line silently removes the previous IdentityGuard Desktop for Microsoft Windows installation, while retaining the offline data.

The second line installs the new version of IdentityGuard Desktop for Microsoft Windows, using the MSI file appropriate for your operating system and the transform file that specifies your modifications to the base installer.

- 2** Save the BAT file with a name like `IG102Install.bat`.
- 3** Copy the BAT file to a shared network directory.
- 4** Run the BAT file from the command line or as part of a larger deployment procedure.

#### Method 2:

- 1** To uninstall, use the following Windows Installer service command-line option:  
`msiexec /x <Product key> REMOVEWIGLOFFLINEKEY=0`



#### Note:

To find the product key, open `setup.ini` and then copy the `ProductCode` in Notepad. For example,  
`ProductCode={A123456F-4C812-7899-BA3E-01AA12345678}`

---

or

for a 64-bit installation:

```
msiexec /x <path>\eigdsktp64.msi REMOVEWIGLOFFLINEKEY=0
```

for a 32-bit installation:

```
msiexec /x <path>\eigdsktp32.msi REMOVEWIGLOFFLINEKEY=0
```

where:

`<path>` is the path to the `eigdsktp32.msi` file



#### Note:

Please note that starting with Windows Installer 3.0, `/x` options can be replaced with `/uninstall`, so there could be more variants of the above command-line examples.

---



# Troubleshooting

This section includes information about troubleshooting resources.

- [“Logging” on page 122](#)
- [“Loss of Entrust credential provider after a reboot” on page 124](#)
- [“Error messages” on page 125](#)

# Logging

Your installation of Entrust IdentityGuard Desktop for Microsoft Windows generates logging information for the desktop client and for the fingerprint enrollment client.

## Logging for the desktop client

By default, all information is recorded in the Windows event log. You can view the authentication activities in the Windows Event Viewer.

When you need to enable logging (for example, if requested by Entrust support), Entrust IdentityGuard Desktop for Microsoft Windows can write logs to a log file. You enable the logging utility by changing the `EnableEIGLogger` and `EIGLoggerCompleteFilename` registry settings. For information about these registry settings, see ["EnableEIGLogger" and "EIGLoggerCompleteFilename" on page 148](#).

## Logging for the fingerprint enrollment client

Logging for the fingerprint enrollment client is disabled by default. Enable logging when requested by Entrust support or to troubleshoot the installation.

### To enable logging for the fingerprint enrollment client

- 1 Locate the `ConfigureLogging.ini` file in your installation. By default, the file is located in the following directory:

```
<install_dir>\Entrust\IdentityGuard Fingerprint Enrollment Client
```

If the file does not exist, create the file using a text editor and add the following text in the file.

```
/* How to configure logging with this file.*/
/*
Enable: 0,do not generate logging file. 1, generate logging
file.
DebugFlags: Displayed error level. The values should be
selected from
"Error,Warning,Trace,Verbose,Detailed1,Detailed2,Detailed3".
LogFile: File path, please create the file folder manually
before collecting logging file. e.g. "c:\temp\BioSDK.log"

*/
[LoggingConfiguration]
Enable=0
```

```
DebugFlags=Error
```

```
LogFile=c:\temp\SDK.log
```

- 2** To enable logging, change the `Enable` value from 0 (no logging) to 1 (generate logs), as shown below:

```
Enable=1
```

- 3** Change the `DebugFlags` value to the logging level you require, for example:

```
DebugFlags=Detailed3
```

- 4** Change the `LogFile` value to the location in which you want to save the log and the file name you want to use for the log, for example:

```
LogFile=C:\temp\fingerprintEnroll.log
```

- 5** Save and close the file.

- 6** Make a copy of the `ConfigureLogging.ini` file and put it in  
<install\_dir>\Entrust\IdentityGuardDesktop\1033.

Log files are generated for the fingerprint enrollment client as long as logging remains enabled.

# Loss of Entrust credential provider after a reboot

After installing Entrust IdentityGuard Desktop for Windows and performing a reboot, the user sees only the regular Windows provider and not the Entrust IdentityGuard credential provider.

This may occur if another credential provider filter conflicts with the Entrust credential provider filter. When multiple credential provider filters try to filter out each other, the Microsoft login framework discards all other credential providers and displays only the default credential provider.

## To ensure access to the Entrust IdentityGuard Desktop provider if not displayed

- 1 Remove other credential provider filters, if any.

You can find these in the Windows registry at the following location:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\
```

- 2 Follow the instructions on the Microsoft page “How to disable additional credential providers” at <https://social.technet.microsoft.com/Forums/windows/en-US/9c23976a-3e2b-4b71-9f19-83ee3df0848b/how-to-disable-additional-credential-providers?forum=w8itprosecurity>.

# Error messages

This section provides a detailed table of all error messages and event logs, as well as solutions and ways to work around them.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_CARD_SUPERSEDED	Entrust IdentityGuard authentication was not successful. The grid you are using is no longer active. Please contact your Entrust IdentityGuard administrator.	The user's grid card is no longer active. Activate or replace the grid card.
IDES_AUTH_INVALID_CHALLENGE	Entrust IdentityGuard authentication was not successful. You entered an incorrect response. Please try again.	There was an invalid response to the challenge set. The user should try again.
IDES_AUTH_INVALID_PIN	Entrust IdentityGuard authentication was not successful. The temporary PIN is incorrect. Please try again.	There was an invalid temporary PIN used to authenticate. The user should try again.
IDES_AUTH_NO_ACTIVE_CARDS	Entrust IdentityGuard authentication was not successful. You do not have an active grid. Please contact your Entrust IdentityGuard administrator.	The user must be assigned an active grid card.
IDES_AUTH_NO_VALID_CARDS	Entrust IdentityGuard authentication was not successful. You do not have a valid grid. Please contact your Entrust IdentityGuard administrator.	The user must be assigned a valid grid card.
IDES_AUTH_OFFLINE_CHALLENGE_GENERAL_ERROR	Entrust IdentityGuard authentication was not successful because of a cryptographic error. Make sure you have a Cryptographic Service Provider installed on your computer.	Ensure the user has a Cryptographic Service Provider (CSP) installed on their computer.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_OFFLINE_CHALLENGE_LOCKOUT	Entrust IdentityGuard authentication was not successful. Your account was locked out because of too many invalid attempts. Use an offline temporary PIN or Q&A to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	The offline grid challenge set is locked. The user should use an offline temporary PIN to login or try to login when their computer is connected to the network.
IDES_AUTH_OFFLINE_INVALID_PIN_AND_LOCKOUT	Entrust IdentityGuard authentication was not successful. The offline temporary PIN is incorrect. Your account was locked out because of too many invalid attempts. Try again after the lockout time expires or use your grid or Q&A to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	The user is now locked out because of too many invalid offline temporary PIN responses. The user should try again after the lockout time expires or use their grid to login. The user may also try to login when the connection to the Entrust IdentityGuard Server is re-established.
IDES_AUTH_OFFLINE_INVALID_QA_RESPONSE_AND_LOCKOUT	Entrust IdentityGuard authentication was not successful. You entered an incorrect response. Your account was locked out because of too many invalid attempts. Use an offline temporary PIN or your grid to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	The user has entered too many wrong answers during offline Q&A. The user should use an offline temporary PIN to login or try to login when their computer is connected to the network.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_OFFLINE_INVALID_RESPONSE_AND_LOCKOUT	Entrust IdentityGuard authentication was not successful. You entered an incorrect response. Your account was locked out because of too many invalid attempts. Use an offline temporary PIN or Q&A to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	The user is now locked out because of too many invalid responses. The user can use their offline temporary PIN to login or wait until a connection to the Entrust IdentityGuard Server is re-established.
IDES_AUTH_OFFLINE_PIN_GENERAL_ERROR	Your temporary PIN could not be authenticated because of a cryptographic error. Make sure you have a Cryptographic Service Provider installed on your computer.	Ensure the user has a Cryptographic Service Provider (CSP) installed on their computer.
IDES_AUTH_OFFLINE_PIN_LOCKOUT	Entrust IdentityGuard authentication was not successful. Your account was locked out because of too many invalid attempts. Try again after the lockout time expires or use your grid or Q&A to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	The offline temporary PIN is locked out so the user should try again after the lockout time expires, use the grid to login, or try to login when their computer is connected to the network.
IDES_AUTH_OFFLINE_QA_CHALLENGE_LOCKOUT	Entrust IdentityGuard authentication was not successful. Your account was locked out because of too many invalid attempts. Use an offline temporary PIN or your grid to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_ONLINE_CHALLENGE_GENERAL_ERROR	Entrust IdentityGuard authentication was not successful. Entrust IdentityGuard has returned an error. Please contact your administrator.	Entrust IdentityGuard Server has returned an error or non-fault SOAP error. Check that the IdentityGuard server is operational.
IDES_AUTH_ONLINE_INVALID_PIN_AND_LOCKOUT	Entrust IdentityGuard authentication was not successful. The temporary PIN is incorrect. You are locked out because you entered an incorrect response too many times. Please contact your Entrust IdentityGuard administrator.	The user is now locked out because of too many invalid temporary PIN responses.
IDES_AUTH_ONLINE_INVALID_RESPONSE_AND_LOCKOUT	Entrust IdentityGuard authentication was not successful. You entered an incorrect response. You are locked out because you entered an incorrect response too many times. Please contact your Entrust IdentityGuard administrator.	The user is now locked out because of too many invalid responses.
IDES_AUTH_ONLINE_LOCKOUT	Entrust IdentityGuard authentication was not successful. You are locked out because you entered an incorrect response too many times.	Please contact your Entrust IdentityGuard administrator.
IDES_AUTH_ONLINE_PIN_GENERAL_ERROR	Your temporary PIN could not be authenticated. Entrust IdentityGuard has returned an error.	Please contact your Entrust IdentityGuard administrator.
IDES_AUTH_PIN_EXPIRED	Entrust IdentityGuard authentication was not successful. The temporary PIN you are using has expired. Please contact your Entrust IdentityGuard administrator.	Assign a new temporary PIN to the user, since their current temporary PIN has expired.



**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_PIN_MAX_US ES	Entrust IdentityGuard authentication was not successful. The temporary PIN you are using has reached maximum uses. Please contact your Entrust IdentityGuard administrator.	Assign a new temporary PIN to the user, since their current temporary PIN has reached its maximum uses.
IDES_AUTH_SYSTEM_ERR OR	Entrust IdentityGuard authentication was not successful. Entrust IdentityGuard has returned a system error.	Please contact your Entrust IdentityGuard administrator.
IDES_AUTH_USER_NO_CH ALLENGE	Entrust IdentityGuard authentication was not successful. Please cancel the Entrust IdentityGuard authentication dialog and try to login again.	The Entrust IdentityGuard Server returned a USER_NO_CHALLENGE error. The user should try and login again.
IDES_CANT_REACH_IG_S ERVER	The Entrust IdentityGuard Server cannot be reached.	Please contact your Entrust IdentityGuard Administrator.
IDES_NO_ACTIVE_TOKEN	Entrust IdentityGuard authentication was not performed. You do not have any active tokens.	Please contact your Entrust IdentityGuard administrator.
IDES_NO_CHALLENGE_IG _SYSTEM_ERROR	Entrust IdentityGuard authentication was not performed. Entrust IdentityGuard has returned a system error. Please contact your Entrust IdentityGuard administrator.	Entrust IdentityGuard Server has returned a system error.
IDES_NO_CHALLENGE_OF FLINE_LOCKOUT	Entrust IdentityGuard authentication was not performed. Your account was locked out because of too many invalid attempts. Try again after the lockout time expires. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	Both offline temporary PIN and challenge set are locked. The user should try again after the lockout time expires or login when the computer is connected to the network.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_NO_CHALLENGE_ONLINE_LOCKOUT	Entrust IdentityGuard authentication was not performed. Your account is currently locked. Please contact your Entrust IdentityGuard administrator.	Get challenge set failed due to lockout error.
IDES_NO_CHALLENGE_SET_OFFLINE	Entrust IdentityGuard authentication was not performed. There are no offline challenges saved for you in this computer. Please login to your computer when it is connected to the network.	Both offline temporary PIN and challenge set data are not available for the Entrust IdentityGuard user.
IDES_NO_CHALLENGE_SET_ONLINE	Entrust IdentityGuard authentication was not performed. Entrust IdentityGuard has returned an error.	Please contact your Entrust IdentityGuard administrator.
IDES_NO_OFFLINE_CHALLENGE_SET	Offline grid challenge authentication is not available. Please use an offline temporary PIN or use offline Q&A to authenticate. Offline grid challenge authentication will be available once you are authenticated to the Entrust IdentityGuard Server online using a grid challenge response.	User has offline temporary PIN but no offline challenge set. This message is displayed when the user wants to switch to use the grid for authentication.
IDES_NO_QA_CHALLENGE_SET_OFFLINE	Entrust IdentityGuard authentication was not performed. There are no Q&A challenges saved for offline use for this account. You can answer a Q&A challenge for later offline use the next time you log in online. Use an offline temporary PIN or your grid to login. You may also try to login when the connection to the Entrust IdentityGuard Server is re-established.	Q&A can only be used offline after the user has successfully answered a Q&A challenge while online. The user must use another method to authenticate while offline.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_NO_QA_CHALLENGE_SET_ONLINE	Your account does not have any question and answer pairs. You must set up question and answer pairs before you can answer a Q&A challenge for later offline use. Please contact your Entrust IdentityGuard administrator for instructions. Once your account has question and answer pairs, you can try again the next time you log in online.	The user does not have any Q&A pairs in IdentityGuard server. They must use whatever means are in place in their organization (for example, Entrust IdentityGuard Self-Service Module) to set up their security questions.
IDES_NO_URL_SETTING	Entrust IdentityGuard Authentication was not performed. The Entrust IdentityGuard URL setting is missing from the registry. Please contact your Entrust IdentityGuard administrator.	There is no Entrust IdentityGuard Server URL configured, but Entrust IdentityGuard is mandatory.
IDES_NON_IG_USER_OFFLINE	Entrust IdentityGuard authentication was not performed. Entrust IdentityGuard authentication is mandatory but there are no offline challenges saved for this account. Currently your computer is not connected to the Entrust IdentityGuard Server. Please login when the connection is re-established.	The user is a non-Entrust IdentityGuard user, or this is the first time the user has logged into Entrust IdentityGuard online on this computer, and Entrust IdentityGuard authentication is mandatory.
IDES_NON_IG_USER_ONLINE	Entrust IdentityGuard authentication was not performed. You are not a registered Entrust IdentityGuard user. Please contact your Entrust IdentityGuard administrator.	The user is a non-Entrust IdentityGuard user, but Entrust IdentityGuard is mandatory.
IDES_ONLINE_USER_NOT_UNIQUE	Entrust IdentityGuard authentication was not performed. Your user name was found in multiple groups. Please contact your Entrust IdentityGuard administrator.	If you selected the <b>Group determined by Entrust IdentityGuard Server</b> selection for the group type, this error is displayed if the user is found in multiple groups.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_PVN_CHANGE_INVALID	Entrust IdentityGuard authentication was not successful. The new PVN provided was not of appropriate length.	Please contact your Entrust IdentityGuard administrator.
IDES_PVN_MISMATCH	The PVNs entered are mismatched. Please try again.	Retype so that the two instances of the new PVN match.
IDES_QA_NOT_ENOUGH_QUESTIONS	Your account does not have enough question and answer pairs. You must have at least as many question and answer pairs as the default Q&A challenge size in Entrust IdentityGuard before you can answer a Q&A challenge for later offline use. Please contact your Entrust IdentityGuard administrator for instructions. Once your account has enough question and answer pairs, you can try again the next time you log in online.	The user does not have enough Q&A pairs in IdentityGuard server. They must use whatever means are in place in their organization (for example, IdentityGuard Self-Service Module) to set up more security questions.
IDES_TOKEN_DRIFT	Entrust IdentityGuard authentication was not successful.	Resetting your token may resolve the issue.
IDES_USER_NO_CARD	Entrust IdentityGuard authentication was not performed. You do not have any active grids. Please contact your Entrust IdentityGuard administrator.	Entrust IdentityGuard user does not have a grid card. Entrust IdentityGuard is mandatory.
IDES_USER_SUSPENDED	Entrust IdentityGuard authentication was not performed. You are currently suspended.	Please contact your Entrust IdentityGuard administrator.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDS_CONFIGURE_QA_FAILE	One or more of your answers was incorrect. Your offline question and answer pairs have not been updated. You can try again the next time you log in online.	This warning informs users that they did not answer the security questions correctly while configuring Q&A for offline use. If they had previously answered security questions correctly, the previous answers can be used while offline. Otherwise Q&A will not be available for offline use until the user successfully answers a Q&A challenge while online.
IDS_NO_SUPPORTED_IG_AUTH_	None of the supported authentication types have been configured for your account. Please contact your Entrust IdentityGuard Administrator.	The user must have a grid or token to authenticate to Windows using IdentityGuard.
IDS_OFFLINE_PIN_CUSTOM_MSG	You are trying to authenticate to Entrust IdentityGuard in offline mode. An offline temporary PIN can be used to authenticate to Entrust IdentityGuard when you do not have the grid you normally use to authenticate, or if you normally use a token to authenticate. Contact your Entrust IdentityGuard administrator to receive your offline temporary PIN for this computer.	This help text is displayed when the user clicks <b>What is my offline temporary PIN?</b> when logging in offline.

**Table 4:** Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDS_OFFLINE_QA_MSG	You are trying to authenticate to Entrust IdentityGuard in offline mode. You can use Q&A to authenticate to Entrust IdentityGuard if you do not have the grid you normally use to authenticate, or if you normally use a token to authenticate. Respond with the same answers that you last used on this computer. If you recently changed your questions and answers, respond with your old answers. To update your offline questions and answers, choose to answer a Q&A challenge the next time you log in online.	This help text is displayed when the user clicks <b>How do I use Q&amp;A?</b> when logging in offline.
IDS_ONLINE_PIN_CUSTOM_MSG	A temporary PIN can be used to authenticate to Entrust IdentityGuard when you do not have the grid or token that you normally use to authenticate. Contact your Entrust IdentityGuard administrator to receive your temporary PIN.	This help text is displayed when the user clicks <b>What is my temporary PIN?</b> when logging in online.

## Customizing the installation package

This chapter contains the worksheets for the **Entrust IdentityGuard Desktop Custom Installation** wizard. For details about how to install and configure Entrust IdentityGuard Desktop for Microsoft Windows, see [“Installing and configuring Entrust IdentityGuard Desktop for Microsoft Windows”](#) on page 71

This chapter contains the following sections:

- [“Entrust IdentityGuard Server information worksheet”](#) on page 136
- [“Configure group type worksheet”](#) on page 137
- [“Configure options for Windows Login”](#) on page 138
- [“Configure options for offline Windows Login”](#) on page 139
- [“Include additional certificates worksheet”](#) on page 143
- [“Include additional registry values worksheet”](#) on page 144

# Entrust IdentityGuard Server information worksheet

Use this worksheet to plan the Windows domains and Entrust IdentityGuard Server URLs to add when you are installing the Windows Login feature using the **Entrust IdentityGuard Desktop Custom Installation** wizard.

**Table 5:** Entrust IdentityGuard Server information worksheet

Windows domain name	Entrust IdentityGuard Server URL(s)



# Configure group type worksheet

Use this worksheet to plan which type of group to use for the Windows Login feature authentication, when you are customizing the **Entrust IdentityGuard Custom Installation** wizard.



**Note:**  
You can configure only one group type.

**Table 6:** Configure group type worksheet

Group options	Required (Circle one)
Group determined by Entrust IdentityGuard Server	Yes No
Use Windows domain as Entrust IdentityGuard group	Yes No
Use this group:	(Add group name)

## Configure options for Windows Login

Use this worksheet to plan the Windows Login feature options to include in the **Entrust IdentityGuard Custom Installation** wizard.

### Table 7: Configure Windows Login options worksheet

Windows Login options	Required (Circle one)
Authentication to Entrust IdentityGuard is mandatory?	Yes No
Authentication to Entrust IdentityGuard when computer is being unlocked?	Yes No
Enable Q&A for offline authentication?	Yes No
Customize a message instructing the user how to use a temporary PIN:	Add text below:

# Configure options for offline Windows Login

Use this worksheet to plan which Windows Login feature offline options you want to include in the **Entrust IdentityGuard Custom Installation** wizard.

**Table 8:** Configure Windows Login offline options worksheet

Windows Login offline options	Required (Circle one)
Maximum number of challenge attempts after which the computer is locked out:	Yes, use default: 5 No, change default to:
Maximum number of temporary PIN attempts after which the computer is locked out:	Yes, use default of: 5 No, change default to:
Maximum number of Q&A attempts after which the computer is locked out	Yes, use default of: 5 No, change default to:
The offline temporary PIN lock-out time limit in minutes:	Yes, use default of: 15 No, change default to:
Customize a message instructing the user how to use an offline temporary PIN:	Add text below:

# Entrust IdentityGuard Self-Service Module information worksheet

Use this worksheet to plan the Windows domains and Entrust IdentityGuard Self-Service Module URLs to add when you are configuring biometric authentication or the self-service password reset feature using the **Entrust IdentityGuard Desktop Custom Installation** wizard.

**Table 9:**

Self-service password reset options	Required (Circle one)
Enable self-service password reset	Yes No
Specify the text to use for the link to the self-service password reset feature, or us the default string: Forgot your password?	

Record the Windows domains and Entrust IdentityGuard Self-Service Module URLs to add.

**Table 10:** Entrust IdentityGuard Self-Service Module (SSM) information worksheet

Windows domain name	Entrust IdentityGuard SSM URL(s)

# Include additional certification providers worksheet

Use this worksheet to plan the additional certification providers that you want to coexist with Entrust IdentityGuard Certification Provider. You can add this information to the `AllowCredentialProviders.ini` file to pre-fill this information in the **Entrust IdentityGuard Custom Installation** wizard, or you can enter the information directly in the wizard.

For each certification provider, enter a name and the globally unique identifier (ID) provided by the certification provider (also found in the Windows registry).

If you choose to add this information to the `AllowCredentialProviders.ini` file, see ["Adding certification providers from a file" on page 142](#).

**Table 11:** Include additional certification providers worksheet

Certification provider name to add	GUID

## Adding certification providers from a file

If you specify credential providers this file, you see them listed in the **Specify other allowed credential providers** page when you complete the **Entrust IdentityGuard Custom Installation** wizard.

### To add certification providers to the AllowCredentialProviders.ini file

- 1 Navigate to the AllowCredentialProviders.ini file. By default, it is located in the following directory:  
`<installation_directory>\Utilities`
- 2 Open the file for editing in Notepad or another text editor.
- 3 To use the Windows Smart Card Credential Provider, which is already included in the file, remove the semi-colon (;) that precedes the line for this credential provider.
- 4 Add more credential providers in the following format:  
name-GUID  
where  
GUID is the globally unique identifier for the credential provider. You can get this number from your credential provider or from the Windows registry.
- 5 Save and close the file.

# Include additional certificates worksheet

Use this worksheet to plan the additional certificates to include in your installation package when you are customizing the **Entrust IdentityGuard Custom Installation** wizard.

**Table 12:** Include additional certificates worksheet

Certificate to add	Certificate type

# Include additional registry values worksheet

Use this worksheet to plan additional registry values to include in your installation package when you are customizing the **Specify Additional Registry Values** page of the **Entrust IdentityGuard Custom Installation** wizard.

**Table 13:** Include additional registry values worksheet

Additional registry values to add
ROOT:
KEY:
Value Name:
Value Type:
Value Data:
Hexadecimal or Decimal (circle one)
ROOT:
KEY:
Value Name:
Value Type:
Value Data:
Hexadecimal or Decimal (circle one)
ROOT:
KEY:
Value Name:
Value Type:
Value Data:
Hexadecimal or Decimal (circle one)



## Registry settings

This appendix contains information about registry settings used by Entrust IdentityGuard Desktop for Windows.

Registry settings can be modified using the custom installation wizard. See [Step 31 on page 104](#) for details.

Registry settings are grouped by the parent key under which they reside.

- “Registry settings under ‘Domains’” on page 146
- “Registry settings under ‘WIGL’” on page 147
- “Registry settings under ‘DomainsAlias’” on page 155
- “Registry settings under ‘SSM’” on page 157
- “Registry settings under ‘SSMDomains’” on page 159
- “Registry settings under ‘Credential Providers’” on page 160

# Registry settings under ‘Domains’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Entrust\WIGL\Domains

**Table 14:** Domains registry settings

Name	Type	Value
<complete domain name>	REG_SZ	<p>URL of the Entrust IdentityGuard Server. For example:</p> <p>https://ig.example.com:8443/IdentityGuardAuthService/services/AuthenticationServiceV11</p> <p>This value is set by the configuration wizard in the <b>Specify Entrust IdentityGuard Server</b> page.</p> <p>This setting allows users to log on using UPN, for example, user@mydomain.com.</p>
<domain name>	REG_SZ	<p>URL of the Entrust IdentityGuard Server. For example:</p> <p>https://ig.example.com:8443/IdentityGuardAuthService/services/AuthenticationServiceV11</p> <p>This value is set by the configuration wizard in the <b>Specify Entrust IdentityGuard Server</b> page.</p>

# Registry settings under ‘WIGL’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Entrust\WIGL\

**Table 15:** WIGL registry settings

Name	Type	Value
AuthenticationUnlockedDesktop	REG_DWORD	<p>If set to 0, users do not need to perform IdentityGuard authentication when a locked Desktop is unlocked.</p> <p>if set to 1, users need to perform Entrust IdentityGuard authentication when a locked Desktop is unlocked</p> <p>Default is 1</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Logon Options</b> page.</p>
AuthenticateLocalUsers	REG_DWORD	<p>If set to 0, local users can access this computer.</p> <p>If this value is not set to 0, only local users registered on Entrust IdentityGuard can access this computer.</p>
BiometricCustomLogoPath	REG_SZ	<p>This registry setting specifies the path to the customized logo image that can be displayed on the fingerprint scanning screen. The image must be a .BMP file.</p>
CustomLogoPath	REG_SZ	<p>This registry setting specifies the path to the customized logo image that can be displayed on the login screen.</p>
DisableFilter	REG_DWORD	<p>If this setting is missing or is set to 0, the Entrust IdentityGuard Credential Provider Filter filters out all other Credential Providers and only the Entrust IdentityGuard Desktop Credential Provider is shown.</p> <p>If the value is set to 1, the Entrust IdentityGuard Credential Provider Filter is disabled and all Credential Providers in the system are shown. This is not a supported mode of operation and is provided for testing and experimental purposes only.</p> <p><b>Note:</b> Do not change this setting unless required.</p>

Name	Type	Value
DisableSSLRevocationChecking	REG_DWORD	<p>If the setting is missing or the value is set to 0, the revocation status of the SSL certificate is checked.</p> <p>If the value is set to 1, the status of the SSL certificate is not checked.</p> <p>This value is not set by the configuration wizard.</p>
EIGLoggerCompleteFilename	REG_SZ	<p>This setting specifies the name of the log file. By default the file is:</p> <p>C:\EIGLogger.log</p>
EIGLoggerFileSizeForRollOn	REG_DWORD	<p>This setting specifies the rollover size. If the log file size reaches the configured file size, the log files are rolled over.</p> <p>If the value is less than 1 (for example, 0), then the default value is used. A value greater than 128 MB defaults to 128 MB.</p> <p>The default is 2 MB</p>
EIGLoggermaxBackupindex	REG_DWORD	<p>This setting specifies the maximum log files backed up with a rollover.</p> <p>Allowed values are 0-99. A value greater than 99 defaults to 99. Set to 0 to disable log file rollover.</p> <p>The default is 5</p>
EnableCombinedAuth	REG_WORD	<p>Set to 0 to disable CombinedAuthentication.</p> <p>Set to 1 to enable CombinedAuthentication. When set users can authenticate using, grid, token, or Mobile TVS authentication.</p> <p>The default is 0.</p>
EnableCombinedAuthDomainList	REG_SZ	<p>Users can enable the CombinedAuthentication for specific domains using this registry. To do the domain names separated by semi colon (;) to this registry entry.</p> <p>If this setting is not present in the registry or if the value is empty, then all the domains are protected by the CombinedAuthentication.</p>

Name	Type	Value
EnableEIGLogger	REG_DWORD	<p>If the value is set to 0, logging is disabled.</p> <p>If the value is set to 1, logs are written to file.</p> <p>Logging is disabled by default.</p> <p><b>Note:</b> Logging should only be enabled for troubleshooting or if requested by Entrust support. Disable troubleshooting when it is no longer required.</p>
EnablefallbackAuthentication	REG_DWORD	<p>If Mobile TVS authentication is not successful, users have the option to retry Mobile TVS authentication or authenticate using a token, as configured in the Entrust IdentityGuard policy.</p> <p>To enable, set the value to 1.</p> <p>To disable, set the value to 0.</p> <p>Fallback is enabled by default.</p>
EnableManualOTP	REG_DWORD	<p>If set to 0, OTP is delivered automatically to the user's contact information.</p> <p>If set to 1, OTP is available by contacting the Entrust IdentityGuard administrator.</p> <p>Default is 0.</p>
EnableOfflineQA	REG_DWORD	<p>If set to 0, offline question and answer (Q&amp;A) is disabled. Users are unable to see the Q&amp;A interface and are not able to use Q&amp;A to authenticate when the Entrust IdentityGuard Server is unreachable.</p> <p>If set to 1 offline (Q&amp;A) login is enabled.</p> <p>Default is 1.</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Logon Options</b> page.</p>

Name	Type	Value
EnableOnlineTempPINAuth	REG_DWORD	<p>This registry setting specifies whether the <b>Use temporary PIN</b> link is displayed to users.</p> <p>If the value is set to 1, the <b>Use temporary PIN</b> link is displayed on the second-factor login page. Users click the link to be directed to a page on which they can enter a temporary PIN, click a link to find out how to obtain a temporary PIN, or choose to authenticate with a grid.</p> <p>If the value is set to 0, the link is not displayed on the second-factor login page.</p> <p>Default value: 1</p>
EnableOfflineTempPINAuth	REG_DWORD	<p>Set to 0 to disable offline temporary PIN if a user fails to connect to Entrust IdentityGuard Server.</p> <p>If set to 1, the temporary PIN is enabled.</p> <p>The default is 1.</p>
EnablePwdMask	REG_DWORD	<p>Set to 0 to enable password reveal. (The user will need to click on the eye symbol in the password text box.)</p> <p>Set to 1 to disable password reveal.</p> <p>The default is 0.</p>
EnablePwdless	REG_DWORD	<p>Set to 1 to enable the passwordless. When set, if the user is also an Entrust IdentityGuard user, after the first log in the password is cached and the user only needs to provide second factor authentication for subsequent log in attempts.</p>
EnableTVS	REG_DWORD	<p>Set to 0 to disable Mobile TVS authentication. Users will always authenticate using token.</p> <p>Set to 1 to enable Mobile TVS authentication.</p> <p>The default is 1.</p>
EnableUPNUserName	REG_DWORD	<p>If set to 1, users with a UPN with full UPN name to perform second-factor authentication, then log in.</p> <p>If set to 0, users with a full UPN name are not allowed to perform second-factor authentication and then log in.</p> <p>The default is 0.</p>

Name	Type	Value
Group	REG_SZ	<p>This value specifies the user's group. If both this setting and UseWindowsDomainAsGroup are used, this value takes precedence.</p> <p>This value is set by the configuration wizard in the <b>Configure Group Type</b> page.</p>
HTTPConnectTimeLimit	REG_DWORD	<p>Time limit in seconds for connecting to the Entrust IdentityGuard Server.</p> <p>If this value is missing, a value of 10 seconds is used.</p> <p>This value is not set by the configuration wizard.</p>
HTTPReceiveTimeLimit	REG_DWORD	<p>Time limit in seconds for connecting to the Entrust IdentityGuard Server.</p> <p>If this value is missing, a value of 10 seconds is used.</p> <p>This value is not set by the configuration wizard.</p>
HTTPSendTimeLimit	REG_DWORD	<p>Time limit in seconds for connecting to the Entrust IdentityGuard Server.</p> <p>If this value is missing, a value of 10 seconds is used.</p> <p>This value is not set by the configuration wizard.</p>
IGAAuthenticationMandatory	REG_DWORD	<p>If this value is set to 0, unregistered users can access this computer</p> <p>If this value is not set to 0, only users registered on Entrust IdentityGuard can access this computer.</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Logon Options</b> page</p>
LogonTo	REG_SZ	<p>Specifies whether the last login was on the local computer or on the domain.</p>
LogonUser	REG_SZ	<p>Contains the name of the last user to log in.</p>
OfflineChallengeAttemptsAllowed	REG_DWORD	<p>The maximum number of allowed failed grid login attempts. after which the user is locked out of the computer.</p> <p>If this value is missing, 5 is used.</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Offline Options</b> page.</p>

Name	Type	Value
OfflineChallengeResponseCount	REG_DWORD	<p>The number of challenge responses saved for offline authentication.</p> <p>If this value is zero or missing, 5 is used.</p> <p>This value should not be changed.</p>
OfflineLockOutTime	REG_DWORD	<p>The offline temporary PIN lock-out time limit in minutes. If this value is set to zero or missing, 15 minutes is used.</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Offline Options</b> page.</p>
OfflineOTPDownloadHours	REG_SZ	<p>If set to 0, offline token authentication is disabled. Set a decimal value between 1 and 336 to set the lifetime (in hours) that Entrust IdentityGuard Desktop for Windows allows offline token authentication.</p> <p>This value is set by the custom installation wizard in the <b>Configure password-less and offline Token authentication options</b> page.</p>
OfflineQAAAttemptsAllowed	REG_DWORD	<p>The maximum number of allowed failed Q&amp;A login attempts after which the user is locked out of the computer.</p> <p>If this value is missing, 5 is used.</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Offline Options</b> page.</p>
OfflineTemporaryPINAttemptsAllowed	REG_DWORD	<p>The maximum number of allowed failed temporary PIN login attempts after which the user is locked out of the computer.</p> <p>If this value is missing, 5 is used.</p> <p>This value is set by the configuration wizard in the <b>Configure Windows Offline Options</b> page.</p>



Name	Type	Value
OfflineTempPINMessage	REG_SZ	<p>Customizable string displayed in a message box that tells users what an offline temporary PIN is and how to get one.</p> <p>The default message is:</p> <p>You are trying to authenticate to Entrust IdentityGuard in offline mode. An offline temporary PIN can be used to authenticate to Entrust IdentityGuard when you do not have the grid you normally use to authenticate, or if you normally use a token to authenticate. Contact your Entrust IdentityGuard administrator to receive your offline temporary PIN for this computer.</p> <p>An alternate message can be set in the <b>Configure Windows Offline Options</b> page of the configuration wizard.</p>
OnlineTempPINMessage	REG_SZ	<p>Customizable string displayed in a message box telling users what a temporary PIN is and how to get one.</p> <p>The default message is:</p> <p>A temporary PIN can be used to authenticate to Entrust IdentityGuard when you do not have the grid or token that you normally use to authenticate. Contact your Entrust IdentityGuard administrator to receive your temporary PIN.</p> <p>An alternate message can be set in the <b>Configure Windows login Options</b> of the configuration wizard.</p>
UseCustomLogo	REG_DWORD	Specifies whether to use a custom logo.
UseWindowsDomainAsGroup	REG_DWORD	<p>If the value is set to 1, the user's the Windows domain is used as the group name. Otherwise the user's group name is set to the value under Group.</p> <p>This value is set by the configuration wizard in the <b>Configure Group Type</b> page.</p>

Name	Type	Value
UsersExemptedOfflineAuth	REG_SZ	<p>In offline mode configurable 2FA exempt Domain Account for Entrust IdentityGuard Desktop. If the registry keys are added for a domain account, then that domain account is exempted from second factor authentication only in offline mode.</p> <p>To enable this feature add a registry key UsersExemptedOfflineAuth under HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL, then add the below string key pair &lt;name/value&gt; under this key.</p> <p>Name: Domain name</p> <p>Type: String</p> <p>Values: User names exempted from offline 2FA separated by semicolon.</p>

# Registry settings under ‘DomainsAlias’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Entrust\WIGL\DomainsAlias

Domain alias creates additional domain names that point to one domain for Desktop Credential Provider login purposes. For example, if your short domain name is testdomain (for example, ig.testdomain.com-long domain name), you can create another domain name, for example, test4 and have it point to the location of testdomain for Desktop Credential Provider login purpose.

**Table 16: DomainsAlias registry settings**

Name	Type	Value
<name of the domain alias> For example: test4	REG_SZ	<p>This setting specifies the domain name the alias points to. This value should be one of the key name mentioned under registry key</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\Domains for Entrust IdentityGuard Server.</p> <p>For example, the short domain name for ig.testdomain.com is testdomain.</p> <p>In this example, the domain alias name test4 is resolved as testdomain by Entrust Desktop Credential Provider.</p> <p>This optional registry key can contain one or more key-value pairs.</p>

# Registry settings under ‘AllowCPs’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Entrust\WIGL\AllowCPs

**Table 17:** AllowCPs registry settings

Name	Type	Value
<name of the allowed Credential Provider> for example, Smartcard Credential Provider	REG_SZ	This registry setting contains the names and GUIDs of credential providers that are allowed to co-exist with Entrust IdentityGuard Desktop.

# Registry settings under ‘SSM’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Entrust\WIGL\SSM

**Table 18: SSM registry settings**

Name	Type	Value
AllowedURL Suffixes	REG_SZ	<p>A list of custom or additional SSM URLs that you want to make available to the Entrust IdentityGuard Desktop client. URLs must be separated by a semi-colon.</p> <p>The specified URLs will be available to users through the self-service link on the Windows login screen. See <a href="#">“Enabling other self-administration operations, in addition to password reset” on page 164</a> for details.</p> <p>You only need to use this registry setting if you customized SSM with non-default URLs. If you are only using default SSM URLs, the Desktop client already recognizes them, so there is no need to set this registry entry. For details on which URLs can be accessed by the Desktop client, see <a href="#">“List of default URLs that are accessible by clicking the self-service link on the Windows login screen” on page 165</a>.</p> <p>The URL specified here will be appended to the end of the main Self-Service Module URL (for example, <code>https://example.com:8445/IdentityGuardSelfService</code>).</p> <p>Only URLs ending in the specified string (and terminated with a “?” or a “;”) will be allowed.</p> <p>Example:</p> <p>If AllowedURLSuffixes is set to:</p> <p><code>administer/myresetToken</code></p> <p>...then the Desktop client can access:</p> <p><code>https://ssmhost.example.com:8445/IdentityGuardSelfService/administer/myresetToken?query1=abc</code></p> <p>...and:</p> <p><code>https://ssmhost.example.com:8445/IdentityGuardSelfService/administer/myresetToken;JSESSIONID=123465346DF321</code></p> <p>...but not:</p> <p><code>https://ssmhost.com:8445/IdentityGuardSelfService/administer/myresetToken/RemainingURL/url?query1=abc</code></p>

Name	Type	Value
DisallowedURLSuffixes	REG_SZ	<p>The same as AllowedURLSuffixes, except that this list contains URLs that users are <i>not</i> allowed to access through the self-service link on the Windows login screen.</p> <p>You can use this setting to disallow access to custom URLs that you may have added to SSM, or to disallow access to any of the default URLs that are on the 'allowed' list. For a list of allowed URLs, see <a href="#">“List of default URLs that are accessible by clicking the self-service link on the Windows login screen” on page 165</a>.</p> <p>For example, if you want to disallow this URL (which is allowed by default)...</p> <pre>&lt;SSM_URL&gt;/administer/lostToken</pre> <p>...then add &lt;SSM_URL&gt;/administer/lostToken to DisallowedURLSuffixes.</p>
InitialURLSuffix	REG_SZ	<p>The URL associated with the self-service link on the Windows login screen. The URL specified here will be appended to the end of the main Self-Service Module URL (for example, https://example.com:8445/IdentityGuardSelfService).</p> <p>If the value is “/”, the SSM Self-Administration Actions page is used.</p> <p>If the value is a customized password reset suffix or some other suffix provided through this registry value, that page is used. If the complete URL (with suffix) is not reachable, an error message is displayed.</p> <p>For details on customizing the self-service link, see <a href="#">“Enabling other self-administration operations, in addition to password reset” on page 164</a>.</p>

# Registry settings under ‘SSMDomains’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Entrust\WIGL\SSMDomains

**Table 19:** SSMDomains registry settings

Name	Type	Value
<name of a SSM domain> for example, myorg	REG_SZ	This registry setting contains all the user SSM domain names and corresponding base SSM URLs.

# Registry settings under ‘Credential Providers’

Located in HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers

**Table 20:** Credential Providers registry settings

Name	Type	Value
ProhibitFallbacks	REG_DWORD	<p>Set this value to 1 to prevent users from circumventing the requirement to log in with second-factor Entrust IdentityGuard credentials by re-booting in Safe Mode.</p> <p>If this value is not set to 1, it is possible for a user to log in to a computer in Safe Mode and avoid the requirement for Entrust IdentityGuard second-factor credentials. By default, Microsoft only runs Microsoft Credential Provider when starting in Safe Mode.</p> <p>The default setting is 0.</p> <p><b>Attention:</b> By setting this registry key, you will explicitly override the fallback safety mechanism that Windows Vista supplies to troubleshoot configuration errors and malfunctioning Credential Providers. Users may be blocked from login in the event of Credential Provider failure.</p>



## IdentityGuard Desktop client integration with SSM

**Attention:**

To integrate the Entrust IdentityGuard Desktop client with SSM, you must deploy the IdentityGuard Desktop 12.0 for Microsoft Windows to user desktops after you install the Desktop clients.

This appendix contains information about integrating the Entrust IdentityGuard Desktop client with Entrust IdentityGuard Self-Service Module. This integration allows IdentityGuard Desktop client users to perform a limited set of self-service administration operations, including:

- reset an Active Directory domain password
- request a temporary PIN if they have lost a token
- request a temporary PIN if they have lost a grid card
- request token synchronization
- reset a personal verification number (PVN)
- unblock a smart credential PIN

# Desktop client and SSM integration overview

The procedures below describe the main tasks you must perform to integrate the Entrust IdentityGuard Desktop client with the Self-Service Module.

## If you are currently running IdentityGuard Desktop 9.2 or 10.1 (with any patches)

Upgrade to the latest version, as documented in [“Preparing for installation” on page 72](#). As part of this process, you must run the custom installation wizard, where you can enable password reset, and optionally, specify additional registry settings related to the Self-Service Module integration.

For details on enabling password reset only, see [“Enabling Active Directory password reset” on page 163](#).

For details on enabling password reset, as well as other self-service actions, see [“Enabling other self-administration operations, in addition to password reset” on page 164](#).

## If you are currently running IdentityGuard Desktop 10.2, and you have customized the default Self-Service URLs

- 1 Check the default URLs. See [“List of default URLs that are accessible by clicking the self-service link on the Windows login screen” on page 165](#).
- 2 If you have customized any of these URLs to have a new name or path, run the custom install wizard, enable password reset, and on the **Specify Additional Registry Values** page, add your custom URLs in the AllowedURLSuffixes registry setting.

For details on running the custom installation wizard, see [“To create a custom installation package” on page 84](#).

For details on the AllowedURLSuffixes registry setting and other Self-Service Module-related registry settings, see [“Registry settings under ‘SSM’” on page 157](#).

For details on enabling password reset and other self-service options, see [“Enabling other self-administration operations, in addition to password reset” on page 164](#).

- 3 Uninstall the old version from the users' desktops.
- 4 Re-install the new installation package that includes your custom URLs.
- 5 Apply Entrust IdentityGuard Desktop 12.0 for Microsoft Windows to users' desktops.

# Enabling Active Directory password reset

You can enable users of the Entrust IdentityGuard Desktop client to reset their Active Directory domain passwords through the Self-Service Module.

When password reset is enabled, a **Forgot your password?** link is added to the first-factor (Windows) login screen. Users click the link to open a browser window (outside of the desktop) that takes them into the password reset workflow. Users can then reset their password through Self-Service, and then use it on the Windows login screen.

To enable password reset, follow the instructions below.

## To enable access to Active Directory password reset

- 1** Follow the procedure [“To create a custom installation package”](#) to [Step 24 on page 101](#).
- 2** In [Step 24](#), select the **Enable self-service password reset** option. If desired, edit the link text.
- 3** If you enable the password reset feature, in addition to the settings you configure in the custom installation wizard, the password reset feature must be enabled in SSM (see [“Configuring the Self-Service Module settings for password reset” on page 75](#)).

The password reset link in your Entrust IdentityGuard Desktop client will allow users to reach the URLs listed in [“Password reset URLs:” on page 165](#).

# Enabling other self-administration operations, in addition to password reset

If you want, you can give users access to more than just the password reset functionality of Self-Service (see [“Enabling Active Directory password reset” on page 163](#)). To do this, you change the **Forgot your password?** link on the Windows login screen to say something like **User Self-Service**, and then you configure the link point to a locked-down version of the Self-Service's Self-Administration Action page. By default, only the actions that can be safely accomplished without a full login to the desktop are available. Those actions are:

- reset an Active Directory domain password
- request a temporary PIN if they have lost a token
- request a temporary PIN if they have lost a grid card
- request token synchronization
- reset a personal verification number (PVN)
- unblock a smart credential PIN

## Do users need to log in to the Self-Administration Actions page?

Yes. When users click the **User Self-Service** link on the Windows login screen, the Self-Service Module's first-factor login page appears. Users must provide their first-factor credentials to access the page. If users have forgotten their first-factor password, they can skip to the password reset pages in order to obtain a new password.

## How do users access the password reset pages?

To access the password reset pages, users must click the **User Self-Service** link, followed by the **Forgot your password link?** on the Self-Service Module's first factor login page. This brings them to the password reset pages, which ask users for their second-factor credentials, and if they are valid, then allow users to specify a new password.

After obtaining a new password, users can use it to log in to the Self-Administration Actions page.

## Enabling a link to the Actions page, and customizing the links on this page

Follow the instructions below to enable a link to the Self-Administration Actions page, and add or remove links on this page.

## To enable a link to the Actions page, and customize the links on this page

- 1 Follow the procedure [“To create a custom installation package”](#) to [Step 24 on page 101](#).
- 2 Change the **Forgot your password?** link text to **User Self-Service** or another phrase that describes the SSM operations that you want to make available to the IdentityGuard Desktop client.
- 3 Continue through the procedure to [Step 31 on page 104](#). Follow the instructions in this step to add the `InitialURLSuffix` registry setting with the value `“/”`. The slash (`“/”`) indicates that users should go to the Self-Service landing page upon clicking the **User Self-Service** link.

For more information about this registry setting, see [“Registry settings” on page 145](#).

- 4 (Optional.) Still in the custom installation wizard, add the `AllowedURLSuffixes` and `DisallowedURLSuffixes` registry settings. These settings allow you to change which URLs (and corresponding Self-Service actions) can be accessed by clicking the **User Self-Service** link. For details on the `DisallowedURLSuffixes` and `AllowedURLSuffixes` settings, see [“Registry settings under ‘SSM’” on page 157](#).

By default, the following URLs are accessible when you have set the `InitialURLSuffix` to `“/”`.

## List of default URLs that are accessible by clicking the self-service link on the Windows login screen

- Password reset URLs:
  - `<SSM_URL>/authenticate/establishPwdRecoveryIdentity`
  - `<SSM_URL>/authenticate/firstFactorAuthentication`
  - `<SSM_URL>/authenticate/validatePwdRecoveryIdentity`
  - `<SSM_URL>/pwdrecover/recoverPassword`
- Authentication URLs:
  - `<SSM_URL>/authenticate/validateInternalAuthentication`
  - `<SSM_URL>/authenticate/secondFactorAuthentication`
  - `<SSM_URL>/authenticate/validateSecondFactorAuthenticat  
tion`
- Administration URLs:
  - `<SSM_URL>/administer/beginAdministration`
  - `<SSM_URL>/administer/resetToken`
  - `<SSM_URL>/administer/handleResetToken`
  - `<SSM_URL>/administer/lostToken`

- <SSM\_URL>/administer/lostGrid
- PVN reset URLs:
  - <SSM\_URL>/administer/forgottenPVN
- smart credential PIN unblock URLs:
  - <SSM\_URL>/administer/unlockSmartCredential
  - <SSM\_URL>/administer/handleUnlockSmartCredential
  - <SSM\_URL>/administer/performUnlockSmartCredential

where <SSM\_URL> is the Self-Service Module's landing page, by default  
<https://selfservicehost.com:8445/IdentityGuardSelfService>



**Note:**

The authentication, administration and PVN URLs require a first-factor login. The password reset URLs do not require any login.

---

## Examples

### Example 1:

If you want to hide the pages related to tokens, add the `DisallowedURLSuffixes` registry setting through the custom installation wizard, and set it to:

```
/administer/resetToken;/administer/handleResetToken;/administer/lostToken
```

### Example 2:

If you want to make available custom self-service pages that you have created, add `AllowedURLSuffixes` registry setting through the custom installation wizard, and set it to:

```
/customURL1;/customURL2
```

where `/customURL1` and `/customURL2` are URL suffixes that will be appended onto the main SSM URL (<https://selfservicehost.com:8445/IdentityGuardSelfService>). All URLs ending with `/customURL1` and `/customURL2` (terminated with a "?" or a ";") will be accessible. For example:

```
https://myssm.example.com:8445/IdentityGuardSelfService/administer/myresetToken?query1=abc
```

```
https://myssm.example.com:8445/IdentityGuardSelfService/administer/myresetToken;JSESSIONID=123465346DF321
```

## ■ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ■

### A

- administrative install 113, 117
- administrative installation 81
- authentication
  - passwordless 47
- authentication methods
  - grid 36
  - mobile soft token 44
  - OTP 41
    - automatic authentication 41
    - manual authentication 42
  - temporary PIN 59
  - token 38
- AuthenticationUnlockDesktop 147

### C

- challenge
  - validating the response 23
- challenge grid 36, 38, 40, 41, 43
- challenge TVS 45
- Customer support 16

### D

- DisableSSLRevocationChecking 148

### E

- EIGLoggerCompleteFilename 148
- EnableCombinedAuth 148
- EnableCombinedAuthDomainList 148
- EnableEIGLogger 149
- EnablefallbackAuthentication 149
- EnableManualOTP 149
- EnableOfflineQA 149
- EnableOfflineTempPINAuth 150
- EnableOnlineTempPINAuth 150
- EnablePwdless 150
- EnablePwdMask 150

- EnableTVS 150

### G

- Getting help
  - Technical Support 16
- grid
  - challenge 36, 38, 40, 41, 43
- grid authentication 36
- Group 151

### H

- HTTPConnectTimeLimit 151
- HTTPReceiveTimeLimit 151

### I

- IGAAuthenticationMandatory 151
- installation
  - silent 111
  - using the Administrative Install 113
- Installation package
  - available on the network 109
  - available on the Web 110
  - customizing 83
  - testing 107
- installation package
  - testing 107
- IntelliTrust 104

### L

- logging mechanism 82

### M

- Microsoft Windows Installer 81
- MSI file 81, 83
- MST file 81

## O

- offline access 23
- offline token 57
- OfflineChallengeAttemptsAllowed 151
- OfflineChallengeResponseCount 152
- OfflineLockOutTime 152
- OfflineOTPDnloadHours 152
- OfflineQAAttemptsAllowed 152
- OfflineTemporaryPINAttemptsAllowed 152
- OfflineTempPINMessage 153
- OnlineTempPINMessage 153
- OTP authentication 41
- OTP automatic authentication 41
- OTP manual authentication 42

## P

- passwordless authentication 47
- personal verification number 21
- personal verification numbers 58
- PIN 78
- Professional Services 16
- ProhibitFallbacks 160
- PVN. See personal verification numbers

## R

- Registry settings reference 145

## S

- Security Provider
  - troubleshooting 121
- self-signed certificates for large deployments 74
- setup.ini file alternative 113
- silent installation 111

## T

- Technical Support 16
- temporary PIN 78
  - authentication 59
- token
  - challenge-response 21, 39
  - response-only 21, 38
- token authentication 38
- transform file 81

- Troubleshooting 121
- TVS
  - challenge 45
- TVS authentication 44
- typographic conventions 12

## U

- UsersExemptedOfflineAuth 154
- UseWindowsDomainAsGroup 153

## W

- Windows Installer file
  - cached version 81
  - customizing 81
- Windows Installer package 81
- Windows Login
  - general information 19