Entrust

Desktop 13.0 SP7 for Microsoft® Windows®

Administration Guide

Document issue: 2.0

Date of Issue: January 2026

TOC

About

About this guide

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

Revision information

Table 1: Revisions in this document

Document issue and date	Section	Description
Document Issue 2.0 January 2026	"About Entrust Desktop for Microsoft Windows"	Minor corrections to the content for "Login screen user tiles" on page 22.
Document Issue 1.0 December 2025	"About Entrust Desktop for Microsoft Windows"	Added the following new sections: • Face biometrics and passkey/FIDO2 token to the section, "Authentication overview" on page 21. • "Login screen user tiles" on page 22 • "Offline/Off-network login with Entrust Desktop Credential Provider" on page 22. • "Change Password using the Windows Security Screen" on page 24.
	"How Entrust Desktop for Windows works"	Added a new section, "Face Biometric with IDaaS" on page 115
	"Registry settings"	Added a new registry setting, "FaceAuthenticationTimeout" on page 212.

Audience

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

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

- Entrust Identity Enterprise or Identity as a Service
- 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
Bold text (other than headings)	Indicates graphical user interface elements and wizards	Click **Next**.
Italicized text	Used for book or document titles	*Entrust TruePass* 7.0 *Deployment Guide*
Blue text	Used for hyperlinks to other sections in the document	Entrust TruePass supports the use of many types of digital ID.
Underlined blue text	Used for Web links	For more information, visit our Web site at www.entrust.com.
`Courier` type	Indicates installation paths, file names, Windows registry keys, commands, and text you must enter	Use the `entrust-configuration.xml` 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 `entrust.ini` file is located in `<install_path>/conf/security/entrust.ini`.
Square brackets [courier type]	Indicates optional parameters	`dsa passwd [-ldap]`

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 Identity Enterprise Administration Guide* contains information required by the Entrust Identity Enterprise administrator.

For help with Identity as a Service, see the *Identity as a Service Administrator Online Help*.

Obtaining additional documentation

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

https://trustedcare.entrust.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 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 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/support/

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

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

https://trustedcare.entrust.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

Professional Services

The Entrust team assists organizations around the world to deploy and maintain secure transactions and communications with their partners, customers, suppliers and employees. Entrust 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 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/solutions/customer-success

Training

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

https://entrust.com/resources/training-services

1

About Entrust Desktop for Microsoft Windows

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

Overview

Entrust Desktop for Microsoft Windows is a small-footprint client that communicates with the Entrust Identity Enterprise or Identity as a Service. Entrust Identity Enterprise is a server-based software product that authenticates and manages users and their authentication data. Identity as a Service is a cloud based product that authenticates and manages users and their authentication data.

Entrust 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 Desktop for Microsoft Windows is installed are not required to use second-factor authentication to log in.

Entrust 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 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 that 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 Desktop for Microsoft Windows.

Authentication overview

Entrust 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-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 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 Identity Enterprise using Entrust Identity Enterprise Self-Service Server (also called Entrust Identity Enterprise Self-Service Module) or Identity as a Service.
- Mobile Smart Credentials authentication, Identity Assured is a strong out-of-band authentication method where an authentication challenge is sent to a user's mobile. This challenge is signed by the Entrust Mobile Smart Credential app and verified by Entrust Identity Enterprise or Identity as a Service. A user can accept or reject the challenge, which results in either a successful or failed authentication.
- Mobile soft token authentication (TVS), an out-of-band authentication challenge is sent to a user's mobile device.
- Face biometric authentication is sent to a user's mobile device. Face Biometric authentication requires users to respond to a notification sent to their Identity App. A user can accept or reject the challenge, which results in either successful or failed authentication.
- Passkey/FIDO2 authentication for online use. Passkey/FIDO2 authentication can replace the old and traditional way of sign-in with fast and secure login experiences. FIDO2 specifications have multifactor authentication and public key cryptography. Unlike password

authentication, FIDO2 stores information, including biometric authentication data on user devices to prevent attacks.

- 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 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 Entrust Identity Enterprise or Identity as a Service. The list that follows describes how Entrust 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.

Login screen user tiles

After installing Entrust Desktop for Windows, users can switch to a different account after the machine is locked. On the Windows login screen, previously logged-in user accounts are displayed as tiles, allowing users to select and sign in to another account.

Offline/Off-network login with Entrust Desktop Credential Provider

- Users who have logged on to a machine at least once prior to installing Entrust Desktop retain cached credentials.
- After installation, these users can continue to log in to the machine in a disconnected or offline state without needing to first connect to the corporate domain.
- This capability ensures that users can access their machines while traveling or working remotely, even when domain connectivity is unavailable.

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 Desktop for Microsoft Windows will validate.

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:
PCI DSS is supported with only Entrust Identity Enterprise.

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" on page 199.

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 Identity Enterprise or Identity as a Service 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 Identity Enterprise 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 Offline Question and Answer (Q&A) has been configured, they will be able to use the responses stored on their computer to log in.

Change Password using the Windows Security Screen

The Change Password functionality on Windows OS integrates with IDaaS password rules to ensure compliance with organizational security policies.

Users can change their password through the Windows Security Screen (CTRL + ALT + DEL) under the following scenarios:

- Intentional change

  The user presses **CTRL + ALT + DEL** and selects **Change a Password**.
- Forced change

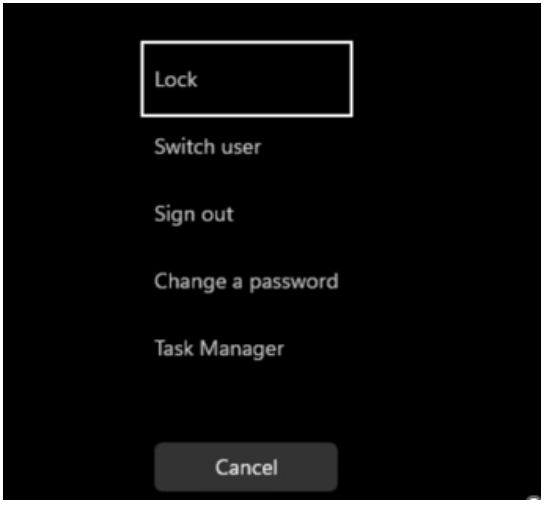
  – The administrator sets **User must change password at next logon**.

  – The user's password has expired.

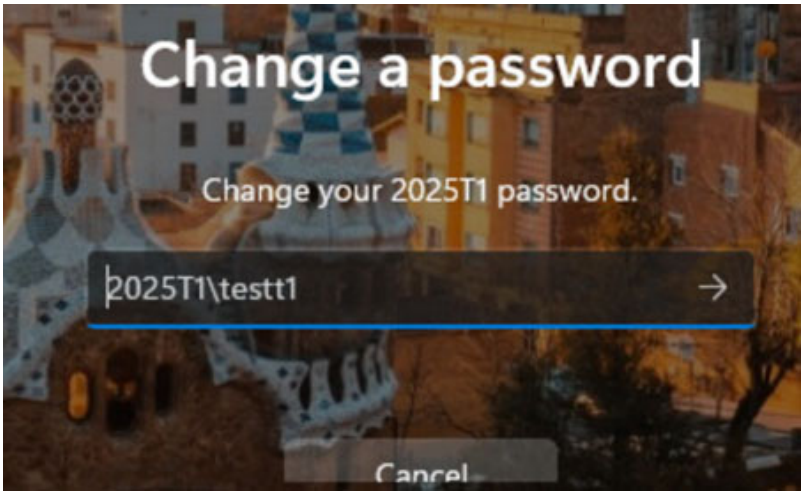
In both cases, IDaaS password rules (for example, length, complexity, history, and restrictions) are enforced.

To change a user password from the Windows Security Screen

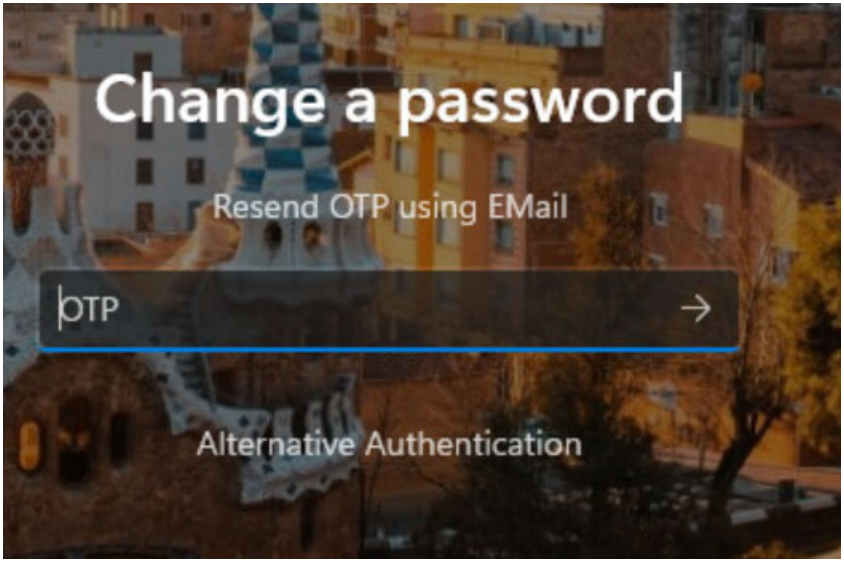
1. Access the Entrust Desktop for Windows resource and enter your username and password.
2. Respond to the second-factor authentication. You are redirected to the resource page after successful authentication.
3. Press **CTRL+ALT+DEL** on your keyboard. The **Windows Security Screen** appears.



4 Click **Change a Password**.

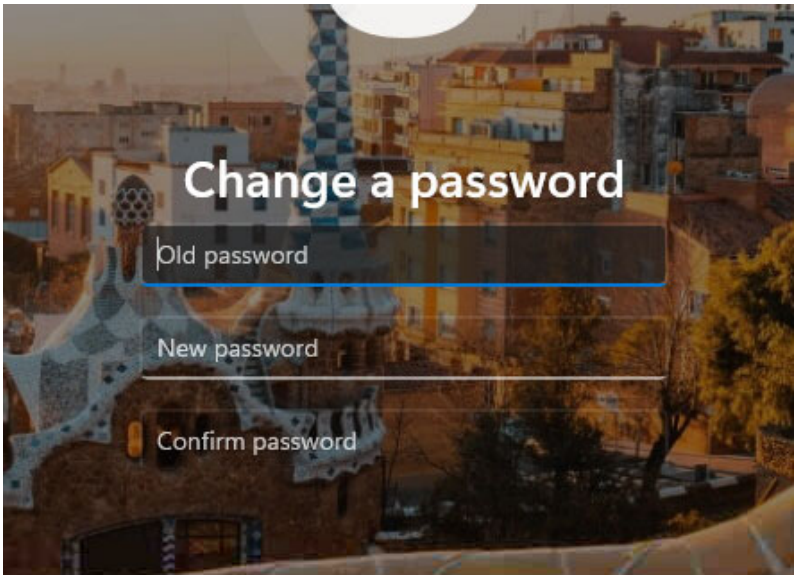


5 Enter your username and then click the arrow (**->**) to move to the next screen. You are prompted to respond to a second-factor authentication.

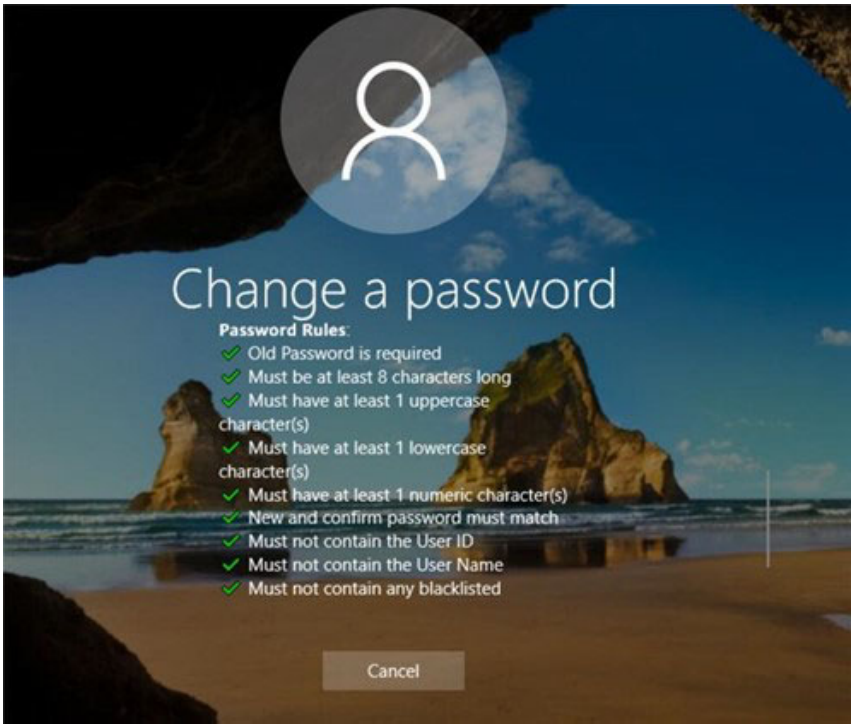


6 Respond to the second-factor authentication.

7 Enter the old password, followed by the new password and then confirm the new password.



8 The new password must meet the IDaaS password rules.



Off-network password reset

The off-network password reset feature allows users to reset their password in a Windows domain-joined laptop. If a Domain user must change their password because it has been compromised or locked, this feature allows them to do so when the laptop is connected to the Internet but not connected to the domain controller.

Note:
If Off-network password reset is enabled and a user logs in to the system in off-network mode, the public network IP of the IDaaS portal gets registered for the user in IDaaS.

Entrust recommends that users connect to the corporate network to cache Windows login password after off-network password reset.

Limitations with off-network second-factor authentication

The following are known limitations with off network second-factor authentication:

- Users, applications, or tools that use a Windows script can use the old password (Device password) to authenticate to the off-network system.
- Microsoft Windows does not call the Entrust Desktop Credential Provider allowing the user to use a cached Windows login (an old password while in off-network mode).
- The following are some of the known usage scenarios:
  - In safe mode, a user can log in to system using old password.
  - User switching using the task manager can use the old password to connect to active user.
  - Users cannot RDP to an off-network system using AD password after a password reset.

    The RDP tool uses Win32 API to authenticate the user credentials so it can understand only cached Windows login passwords.

    To RDP to another system, the user must enter their old password in mstsc tool and then on the target system enter the domain user password to login.

To avoid these limitation, users must connect to the corporate network to cache the Windows login password after a password reset.

Alternate authenticators

Entrust Desktop for Microsoft Windows configured with Identity as a Service authentication can include links to other authenticators on its second-factor login page if the user has more than one authenticator. Users can select an alternative authenticator if they do not have their primary authenticator.

The following authenticators are supported as alternatives:

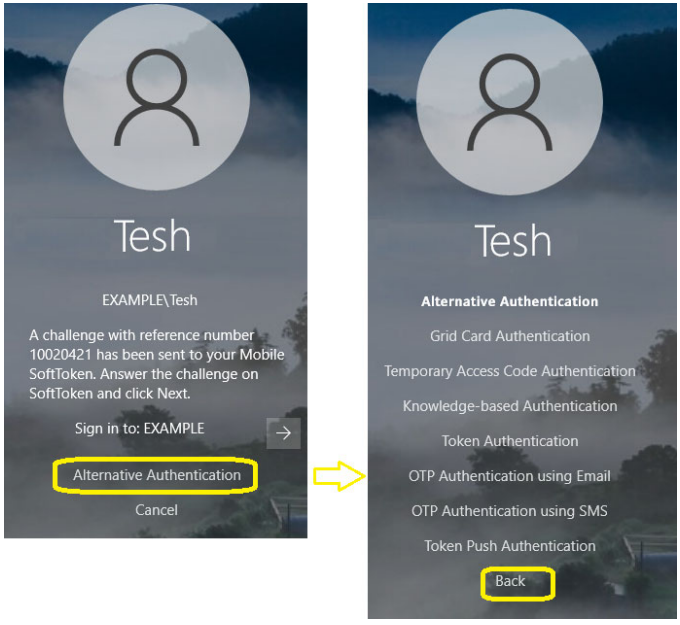
- Online
  - grid
  - token
  - knowledge-based Q&A
  - one-time password (OTP) which supports delivery by SMS, email, and Voice.
  - Mobile smart credential
  - Mobile soft token
  - Temporary Access Code
  - Passkey/FIDO2
  - Face Biometric
- Offline

– grid
– token
– knowledge-based Q&A

Note:
The alternate authenticator link appears on the second-factor authentication screen for login, unlock, and password reset. Offline authentication is only available for login and unlock. Offline authentication does not support password reset.

With IDaaS, Entrust Desktop displays the Alternate Authenticator link on the second-factor authentication screen as shown in Figure 1.

Figure 1: Alternate authenticator link in IDaaS



Deployment and management

To make deployment and management easy, Entrust 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 Desktop for Microsoft Windows software from a specified URL using a Web browser

Administrators use the **Custom Installation** wizard that comes with Entrust 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

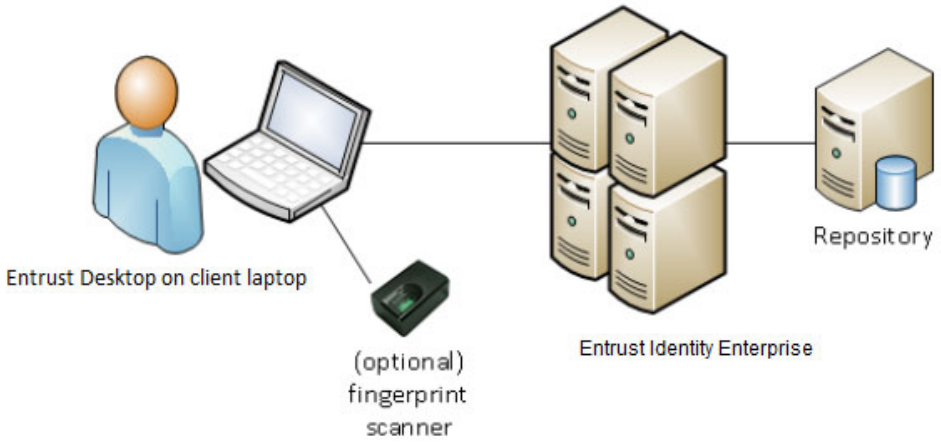
- use existing Microsoft tools to modify the Microsoft registry on the user's desktop.
- create a new installation package to distribute to users by running the **Entrust Custom Installation** wizard again.

Windows Login feature system components

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

Figure 2 on page 32 illustrates the Windows Login basic system components using Entrust Identity Enterprise as an example.

Figure 2: Windows Login system components



Microsoft Windows client

Entrust Desktop for Microsoft Windows is a small-footprint client that communicates with Entrust Identity Enterprise or Identity as a Service. 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 Identity Enterprise or Identity as a Service protection.

Entrust Identity Enterprise

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

Entrust Identity Enterprise is a server-based software product installed in an organization's current infrastructure. It is the main component of the Entrust

Identity Enterprise system. It includes the applications and interfaces required to authenticate and manage users and their authentication data. Entrust Identity Enterprise uses a repository to store user data.

Repository

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

Entrust Identity Enterprise 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 Desktop for Microsoft Windows software

1. Open the Windows **Control Panel** and access **Programs and Features**.
2. The Entrust 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\edccp64.dll
- C:\Windows\System64\edccpfilter64.dll
- C:\Program Files\Entrust\Desktop\1033\edccpenu64.dll
- C:\Program Files\Entrust\Desktop\1033\edccpevenu64.dll

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

2

Installing and configuring Entrust Desktop for Microsoft Windows

Installing and configuring the Windows Login feature of Entrust 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

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

Setting up users

Users must have user IDs in the network and be configured on the Entrust Identity Enterprise or Identity as a Service before they can use Entrust Desktop for Microsoft Windows. The pre-installation and installation sequence is:

- An administrator creates user IDs for users.
- An administrator creates grids in Entrust Identity Enterprise or Identity as a Service (if applicable).
- An administrator assigns a grid, token, PVN, temporary PIN, or Temporary Access Code 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.

Gathering custom installation data

Collect custom installation data related to your organization's Entrust setup. Use the worksheets in "Customizing the installation package" on page 189 to plan the data required for your Entrust Desktop for Microsoft Windows deployment.

Communication between Desktop for Microsoft Windows and the Entrust Identity Enterprise

The Entrust Identity Enterprise implements a Web service for authentication using HTTPS. During configuration, you are asked for the URL of the authentication service running on the Entrust Identity Enterprise or Identity as a Service.

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

The format of the URL is as follows:

```
https://ig.example.com:8443/IdentityGuardAuthService/services/Auth
enticationServiceV13
```

To establish secure SSL communication between the server and Entrust Desktop for Windows client, client computers must have the trusted root certificate from the Entrust Identity Enterprise 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 Desktop for Microsoft Windows installation package" on page 49.

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

- a publicly-trusted SSL certificate such as a certificate from Entrust Certificate Services.

  https://www.entrust.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 Desktop for Microsoft Windows behaves as if Entrust Identity Enterprise is not available.

Instead, use an SSL certificate issued by a public root. That way, each time the SSL certificate used by Entrust Identity Enterprise 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 Desktop Credential Provider 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 “Create a custom installation package” on page 50.

Topics in this section include:

Configuring the Entrust Identity Enterprise or Identity as a Service settings

You must configure the Entrust Identity Enterprise or Identity as a Service information in the **Entrust Desktop Credential Provider Custom Installation** wizard. This information enables the Windows Login feature to communicate securely with the Entrust Identity Enterprise or Identity as a Service for second-factor authentication. You can configure multiple Windows domains with multiple Entrust Identity Enterprise Servers or Identity as a Service. Set up communication with the Entrust Identity Enterprise or Identity as a Service using HTTPS (not HTTP).

If you want to install Entrust Desktop for Windows for Identity as a Service, you must:

1 Add **IntelliTrust Desktop** to Identity as a Service and copy the Application ID for use in the Entrust Desktop Credential Provider Custom Installation wizard.

See 'Integrate Entrust Desktop for Windows' in the *Identity as a Service Online Help* for more information.

2. You must also create a resource rule to protect your resource.
3. In the resource rule, select **External authentication** for first-factor and the required second-factor authenticators.

See the section, "Integrate Identity as a Service Desktop" in the Identity as a Service Administrator Online Help for more information.

Configuring the Self-Service Module settings for password reset

If you want users to be able to reset their Window password and perform other administrative tasks in the Entrust Identity Enterprise 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 Identity Enterprise Self-Service Module Installation and Configuration Guide*.
2. Use the Entrust 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 “Installing for Entrust Identity Enterprise” on page 67.

Configure off-network password reset

Off-network password reset is available only for Identity as a Service directory users only.

To configure off-network password reset, complete the following:

- “Create a first-factor authentication application” on page 41
- “Configure off-network password reset” on page 41

Create a first-factor authentication application

1. Log in to IDaaS.
2. Go to **Resources > Applications**. The **Applications** page appears.
3. Click **Add**. The **Select an Application Template** page appears.
4. Under **API Applications**, click **Authentication API**. The **Add Authentication API** page appears.
5. In the **Application Name** field, type a name for your application.
6. In the **Application Description** field, type a description for your application.
7. Click **Next**.
8. Enable the setting for **Do Not use IP address for Resource Rules Risk Factors**.
9. Click **Submit**.
10. Create a resource rule to protect applications (see the Create resource rules in the Identity as a Service online help for more information).
11. When setting the authentication methods for the resource rule, select **Password** for **First Factor** and deselect all second-factor authentication methods.

Configure off-network password reset

Configure off-network password reset using the Entrust Desktop for Windows custom installation Wizard. See Step 11 on page 58.

Specifying other allowed Credential Providers

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

Configuring for Entrust Identity Enterprise only

Review the following if you are configuring for Entrust Identity Enterprise:

- "Including additional certificates" on page 42
- "Disabling revocation checking" on page 42
- "Configuring the group type" on page 43

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 Identity Enterprise for second-factor authentication. If Entrust Identity Enterprise is not using a self-signed SSL certificate, the trusted CA root certificate that issued the Entrust Identity Enterprise 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 Identity Enterprise 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 "Installing for Entrust Identity Enterprise" on page 67.

Configuring the group type

An Entrust Identity Enterprise 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 Identity Enterprise for second-factor authentication, the group type configured at the Windows desktop must match the group type configured at the Entrust Identity Enterprise.

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

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

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

- **Use Windows domain as Entrust Identity Enterprise 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 Identity Enterprise or Identity as a Service authentication.

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

- **Authentication to Entrust is mandatory**
- **Authentication to Entrust 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** credential provider screen:

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

Note:
Identity as a Service uses Temporary Access Codes Temporary Access Codes can be used to log in when a user cannot access their one-time password (OTP), Grid Card, or token authenticator (for example, if a user has misplaced the mobile device containing their Entrust Soft Token mobile application).

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 Entrust 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 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 Entrust online) then the user is treated as a non-Entrust 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 Desktop Credential Provider 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 Desktop Credential Provider 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 Desktop Credential Provider 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 Desktop Credential Provider 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 Desktop Credential Provider 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 Desktop Credential Provider 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 Desktop Credential Provider 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 Desktop Credential Provider 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 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 98.

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 Desktop for Microsoft Windows installation package

Use the **Entrust Desktop Credential Provider 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 10, Windows Server 2012, Windows Server 2016, and Windows 2019 use `IDG_CP_13.0_win81_Server2019_x086` or `IDG_CP_13.0_win81_Server2019_x064`, as follows:
  - For 64-bit: `<install folder>\Utilities\edcwincustwiz64.exe`
  - For 32-bit: `<install folder>\Utilities\ecdwincustwiz32.exe`

The **Custom Installation** wizard uses a Microsoft Windows Installer file (`MSI`) provided with the Entrust 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 Desktop for Microsoft Windows is delivered as a Windows Installer package (`MSI` file) that you can configure.

The Entrust Desktop for Microsoft Windows ZIP file contains the following file structure in the `IDG_CP_13.0_win81_Server2019_x086` or `IDG_CP_13.0_win81_Server2019_x064` folder:

- `license.rtf`—the Entrust Desktop for Microsoft Windows license.
- `edcdsktp64.msi (or edcdsktp32.msi)`—the Entrust Desktop for Windows and fingerprint enrollment client installer package.
- `setup.ini`—the `setup.exe` configuration file.
- `setup.exe`—the Entrust Desktop setup executable.
- `Utilities` folder
  - `edcwincustwiz64.exe (or edcwincustwiz32.exe)`—the **Entrust Desktop Credential Provider Custom Installation** wizard.
  - `AllowCredentialProviders.ini` —the file you use to specify other credential providers that can coexist in your implementation in addition to Entrust Desktop for Microsoft Windows.

Using the custom installation wizard

The following procedures describe the steps involved in creating a custom installation package with the **Entrust Desktop Custom Installation** wizard.

Create a custom installation package

To prepare for installation, you must download the custom installation package.

To download a custom installation package

1 On any computer running a supported version of Windows, download and extract the required installation file from Entrust Trusted Care (https://trustedcare.entrust.com).

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

Continue with the installation using one of the following procedures:

- “Installing for Identity as a Service” on page 51
- “Installing for Entrust Identity Enterprise” on page 67

Upgrade Entrust Desktop for Microsoft Windows

The installer automatically upgrades Entrust Desktop for Microsoft Windows 12.0, 12.1, or 12.2 to Entrust Desktop for Microsoft Windows version 13.0. It also upgrades the new folder structure and registry structure as follows:

- Existing registry structure: `Software\\Entrust\\WIGL\\Intellitrust`
- New registry structure: `Software\\Entrust\\WIGL\\IDaaS`
- Existing folder structure: `<install_dir>\Entrust\Datacard Desktop\`
- New folder structure: `<install_dir>\Entrust\Desktop\`

Installing for Identity as a Service

Use this procedure to install Entrust Desktop for Windows for Identity as a Service authentication.

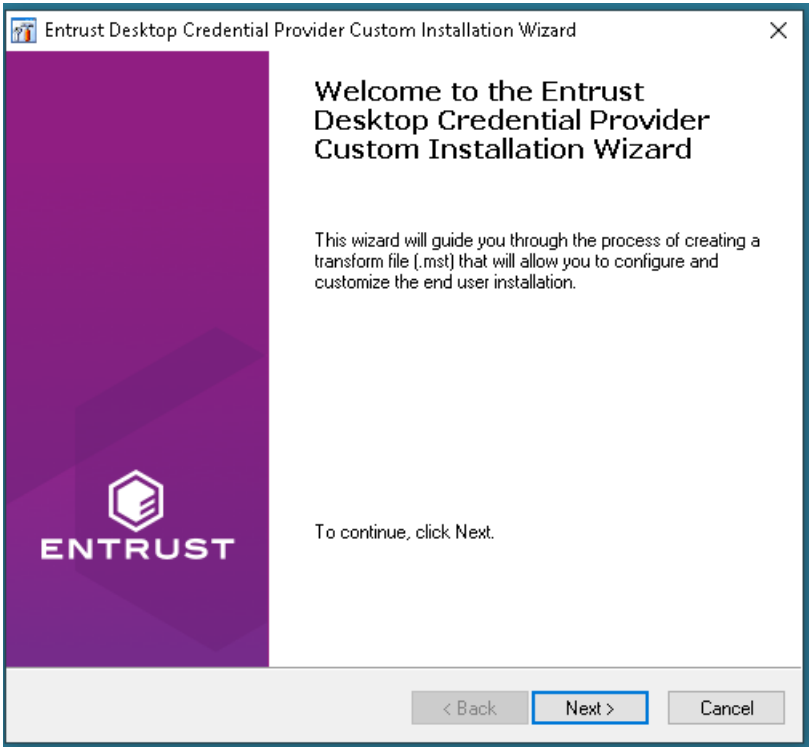
To install for Identity as a Service

1 Launch the **Custom Installation** wizard as follows:

   a Navigate to the `<IDG_CP_13.0_extracted_folder>\Utilities\` folder.

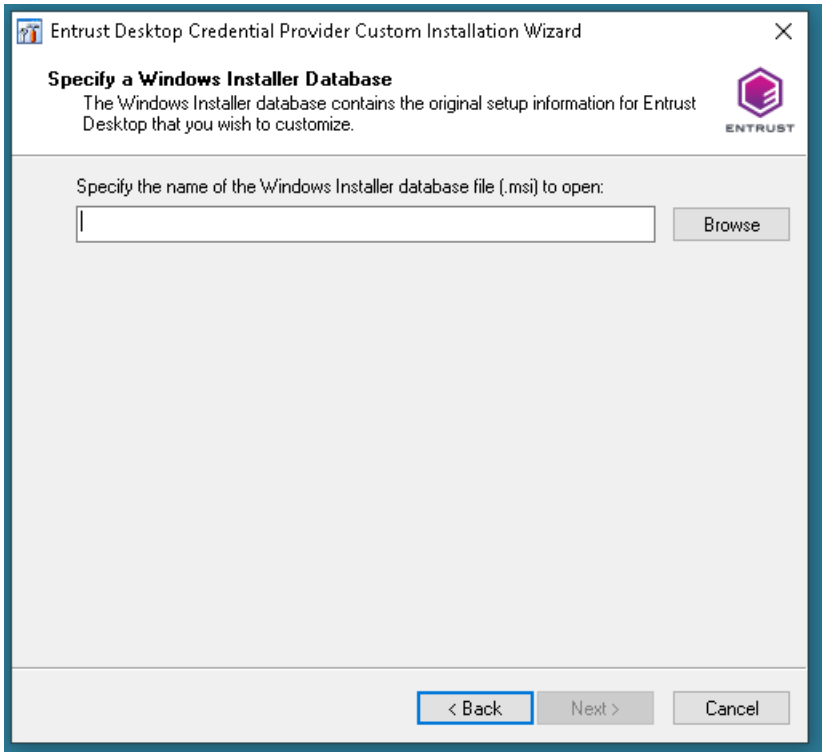
   b Double-click `edcwincustwiz64.exe`. (or `edcwincustwiz32.exe`).

   The **Desktop Setup** wizard appears.



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

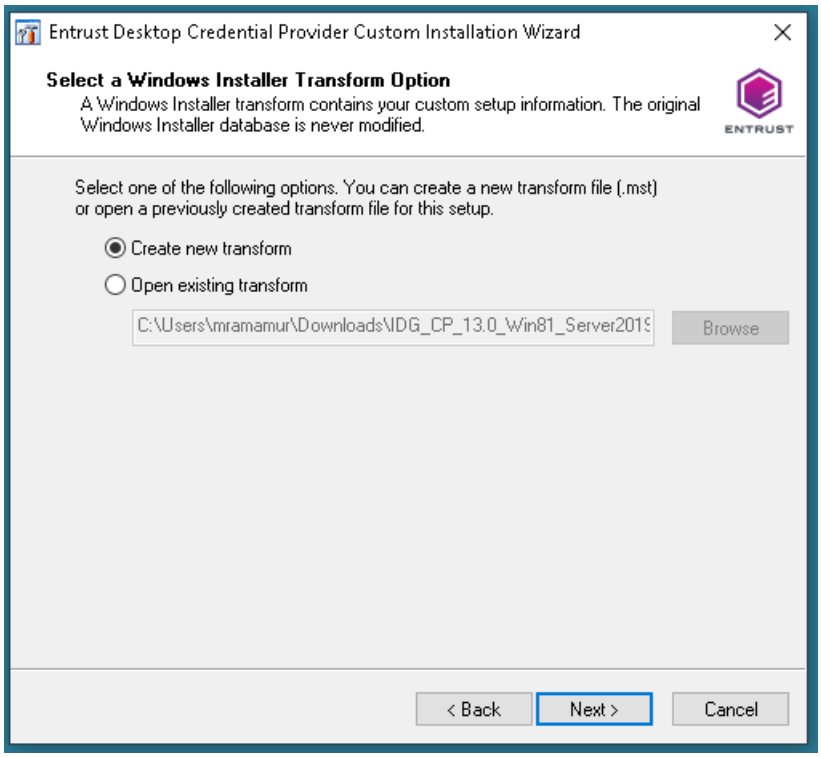
The **Specify a Windows Installer Database** page appears.



3 Enter the path for the Entrust Desktop for Microsoft Windows installation file (`edcdsktp64.msi` or `edcdsktp32.msi`). This file is included with your Entrust Desktop for Microsoft Windows software.

4 Click **Next**.

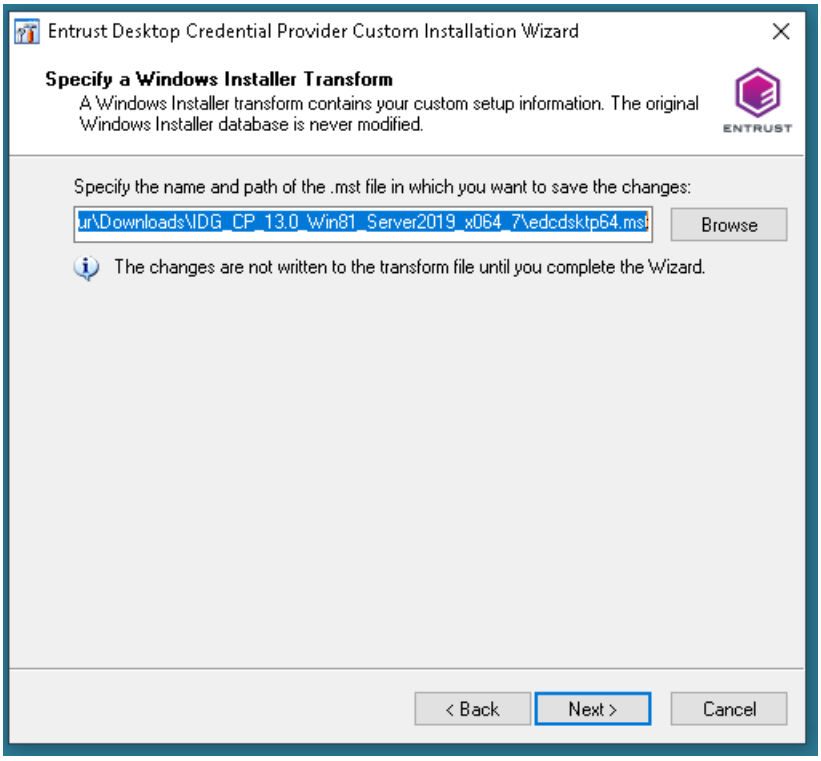
The **Select a Windows Installer Transform Option** page appears.



5 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.

6 Click **Next**.

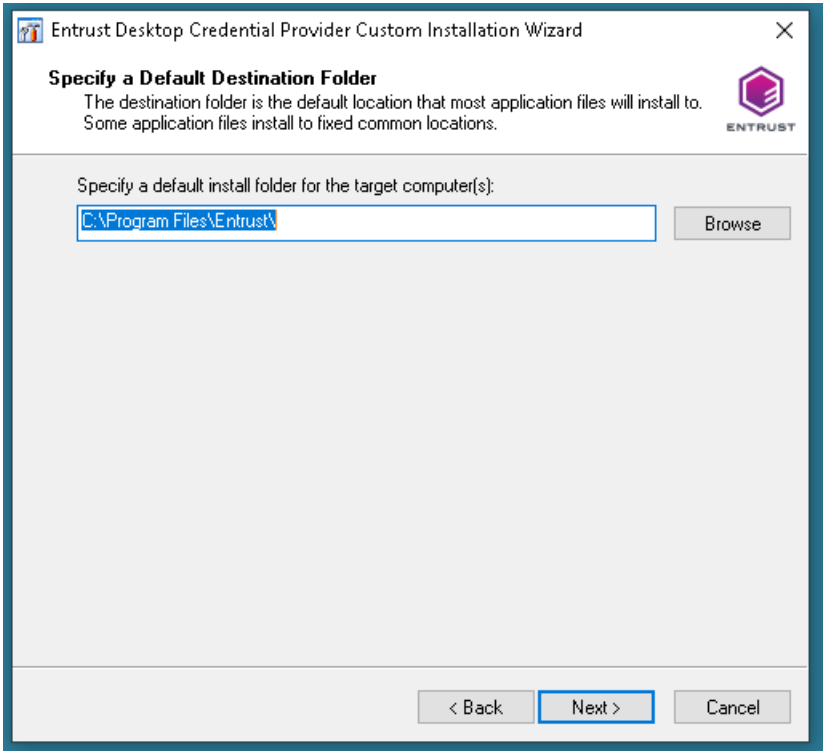
The **Specify a Windows Installer Transform** page appears.



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.

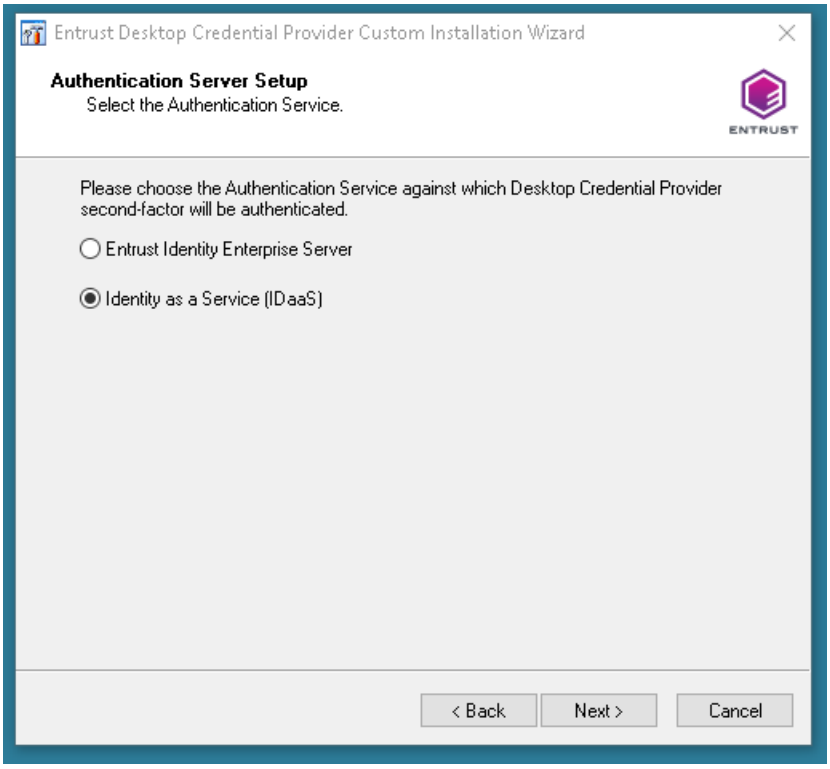
7 If you are creating a new transform file, specify the path and the file name. Browse to the `MST` file in which to save your custom setup information and click **Next**.

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

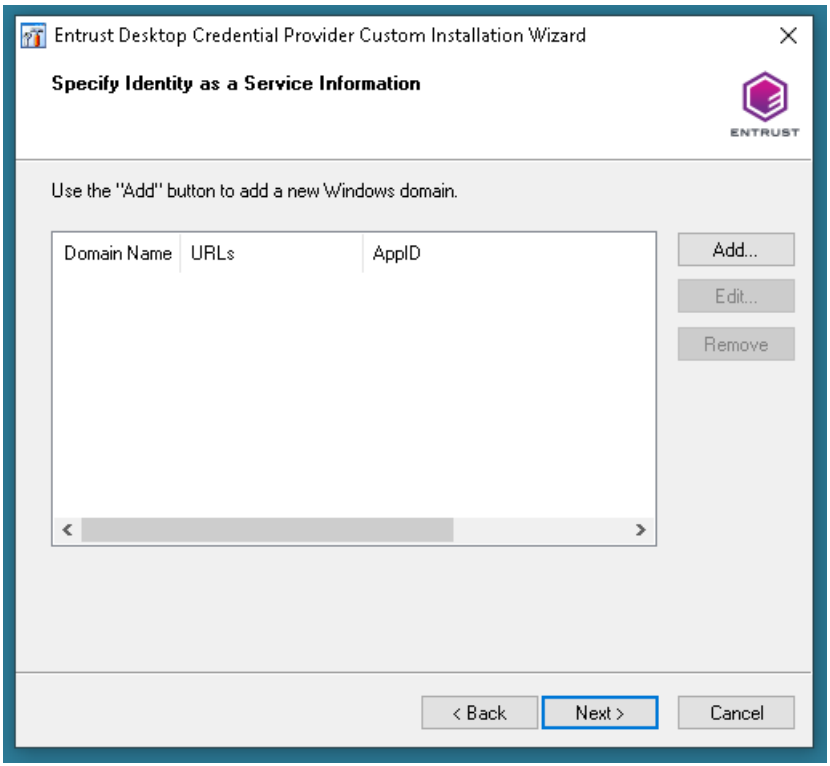


8 Select the default installation folder on the target computer and click **Next**.

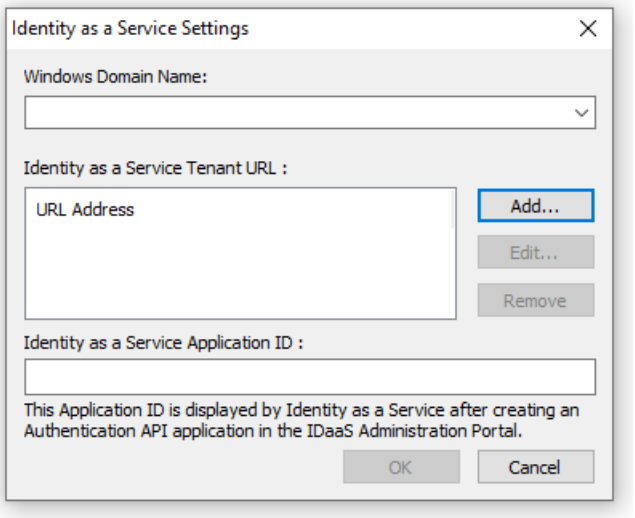
The **Authentication Server Setup** page appears.

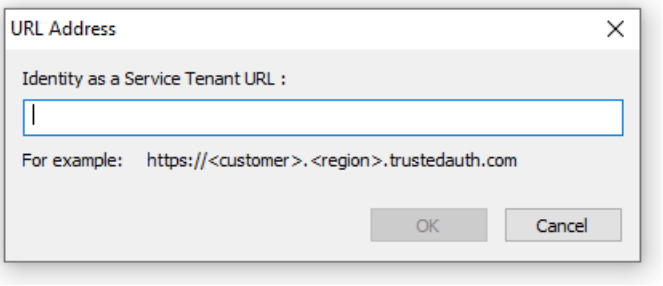


9 Select **Identity as a Service Authentication Service** and then click **Next**.
The **Specify Identity as a Service Information** page appears.



10 Click **Add**. The **Identity as a Service Settings** page appears.

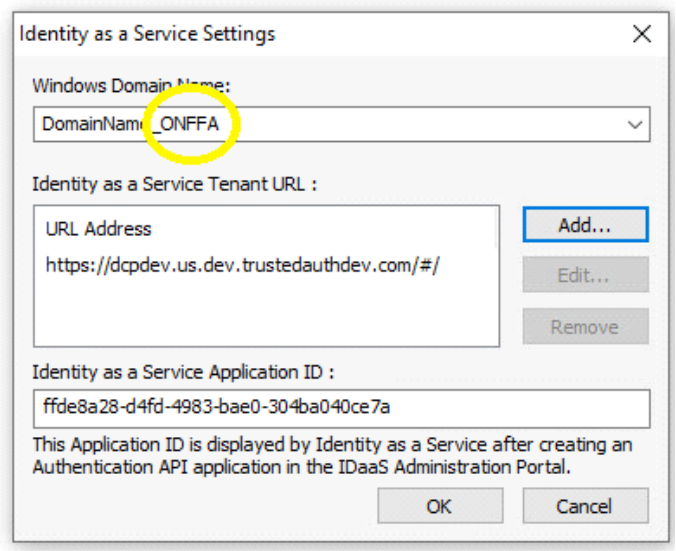




11 Set the **Identity as a Service Settings** as follows:

a Select the **Windows Domain Name** where the client computer is located from the drop-down list. This is the name of the domain in which the user's computer is located, not the domain where Identity as a Service is located.

b To use the off-network password reset option, append **_ONFFA** to the Domain name, for example, `mydomain_ONFFA`.



c Click **Add** to add Identity as a Service Tenant URLs.

d In the **URL Address** dialog box, enter the **Identity as a Service Tenant URL** and click **OK**.

e Enter the first-factor authentication application ID that you created in the section, "Create a first-factor authentication application" on page 41.

f Click **OK** to return to the **Specify Identity as a Service Information** page.

g Click **Add**. The I**dentity as a Service Settings** page appears.

h Select the same Windows domain name as the Off-network reset domain name.

i Do not append `_ONFFA` to the Domain name. Only the domain name should appear. For example: `mydomain`.

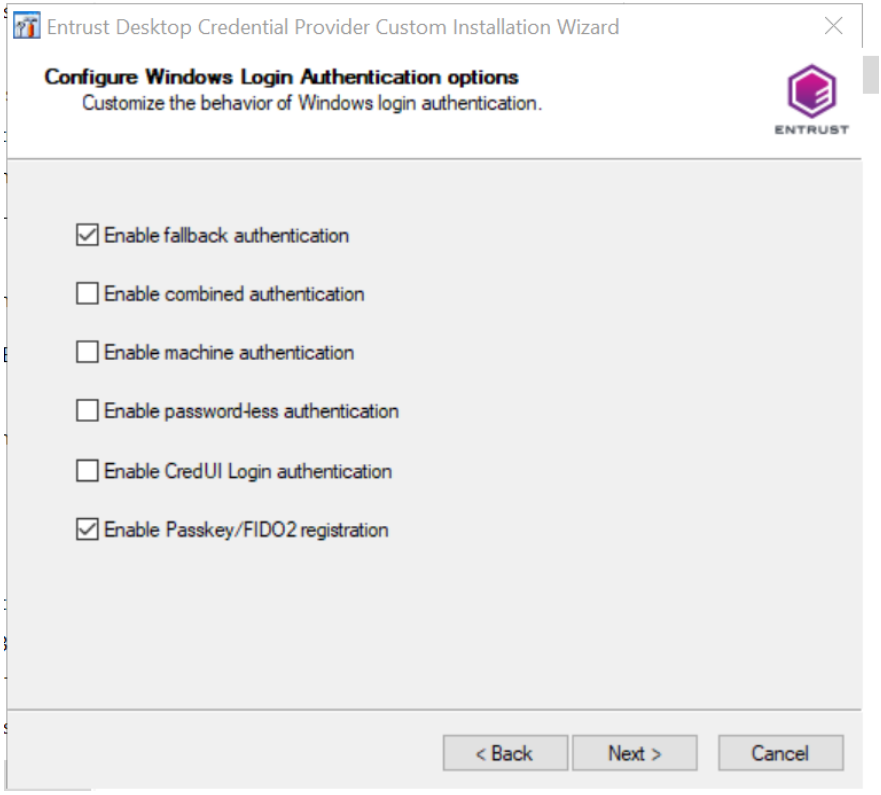
j Click Add to add Identity as a Service Tenant URLs.

k In the URL Address dialog box, enter the I**dentity as a Service Tenant URL** and click **OK**.

l Enter the **IntelliTrust Desktop application ID**. See the section, "Configuring the Entrust Identity Enterprise or Identity as a Service settings" on page 39.

m Click **OK** to return to the **Specify Identity as a Service Information** page.

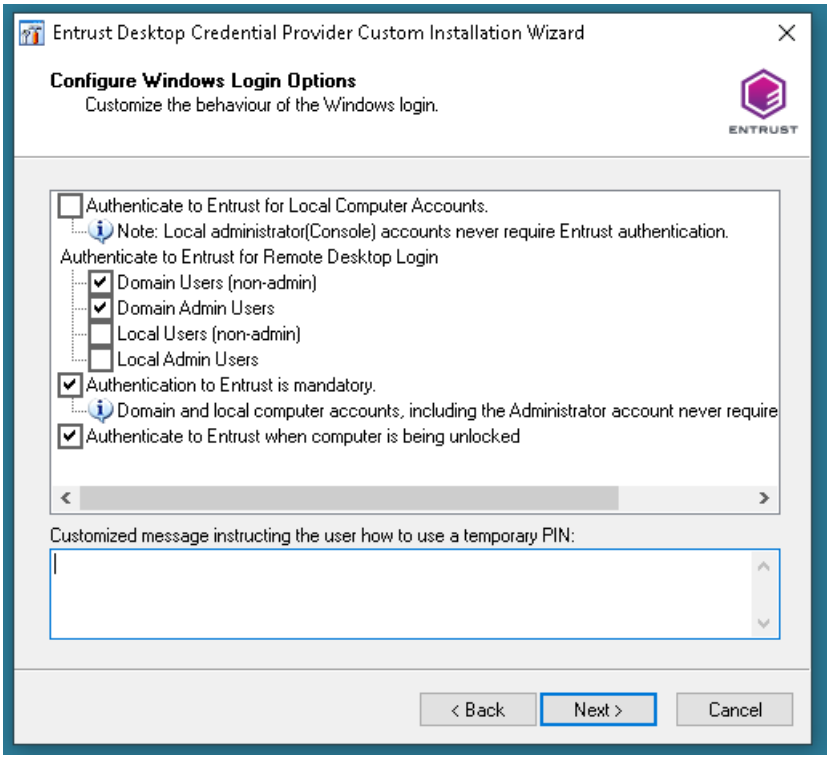
12 Click **Next**. The **Configure Windows Login Authentication options** page appears.



13 Select the following options:

- **a** Select **Enable fallback authentication** if you want to allow users to use an alternate authenticator if their primary authentication method is unavailable.
- **b** Select **Enable combined authentication** if you want if you want first- and second-factor authentication challenges to be evaluated at the same time.
- **c** Select **Passwordless authentication** if you want to skip first factor password authentication.
- **d** Select **Enable CredUI Login authentication** if you want to allows users to authenticate elevated login.
- **e** Select **Enable Passkey/FIDO2 registration** if you want users to register a Passkey/FIDO2 token for second-factor authentication.

14 Click **Next**. The **Configure Windows Login Options** page appears.



15 On the **Configure Windows Login Options** page:

a To require all users to authenticate to Identity as a Service, select **Authentication to Entrust is mandatory**.

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

- To require users to authenticate when unlocking their computers, select **Authenticate to Entrust when computer is being unlocked**. If you deselect this box, users that are not registered in Entrust will be able to log in without a second factor challenge.

16 Click **Next**. The **Configure Windows Login Offline Options** page appears.

a Enter the **Max number of grid attempts after which the computer is locked**.

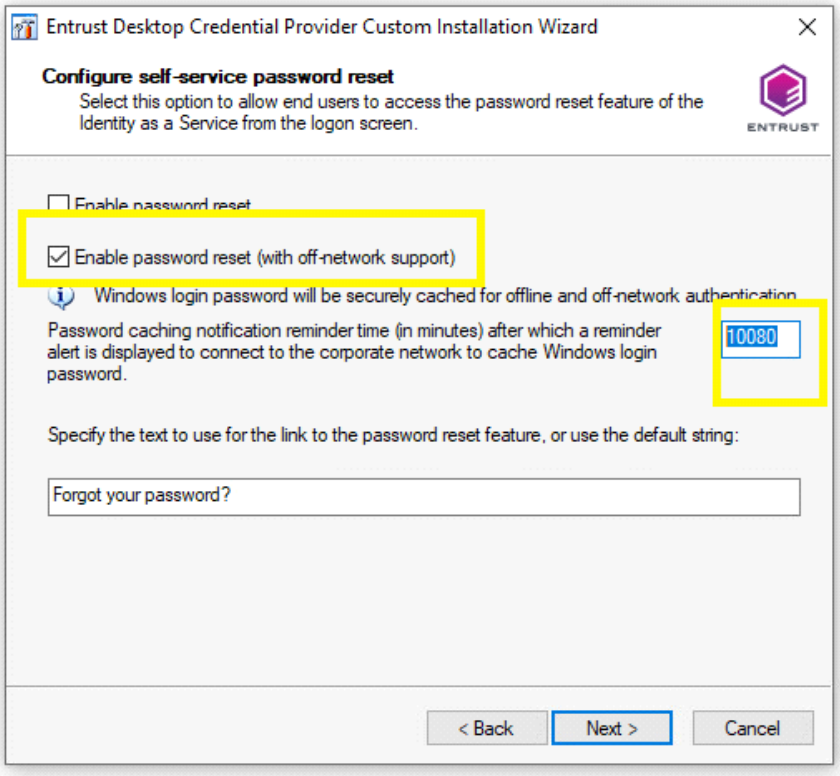
b Enter a value for the **Specify the token download time (in hours)**.

c To enable users to log in to the computer offline using question and answer authentication, **Select Enable Q&A for offline authentication**.

d Enter the **Max number of Q&A attempts after which computer is locked**.

17 Click **Next**. The **Customize the logo on the login screen** page appears.

18 Click **Next**. The **Configure self-service password reset** page appears.



a Selected **Enable password reset (with off-network support)** to allow off-network password reset.

b Enter **Password caching notification reminder time** to set the reminder time (in minutes) for a user to connect to the corporate network to cache the Windows login.

c Enter the text that appears on the password reset link.

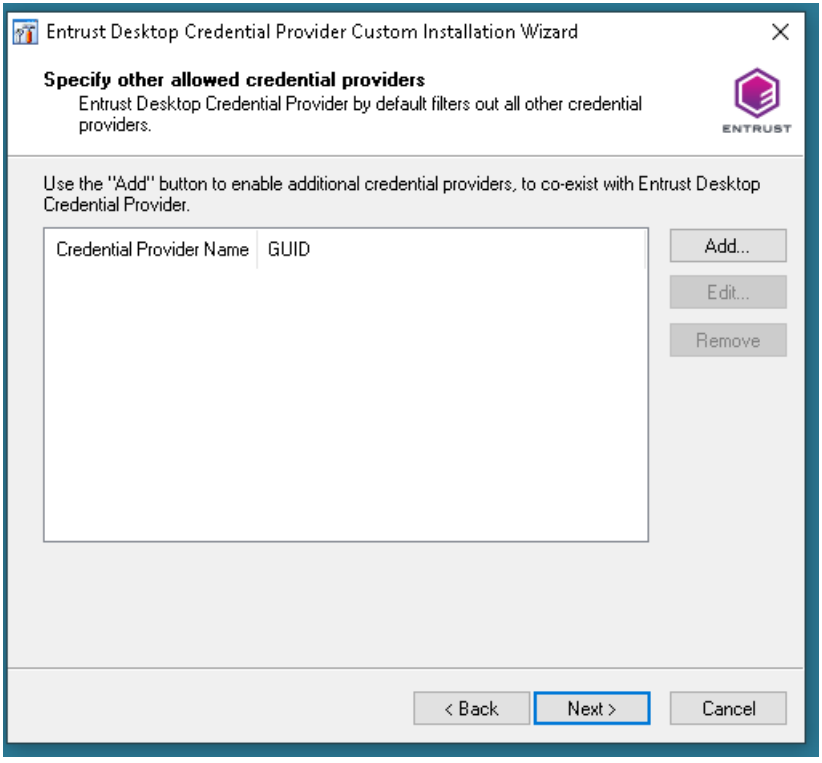
19 If you want users to allow to reset their forgotten passwords, do the following:

a Select **Enable password reset** to allow users to reset their password. When enabled, a *Forgot Password* link appears on the login screen.

Note:
If you enable this feature, you must you must also enable password reset in Identity as a Service. See the following section, **Manage authenticators > Manage password authenticators > Manage password reset** in the *Identity as a Service Administration Online Help.*

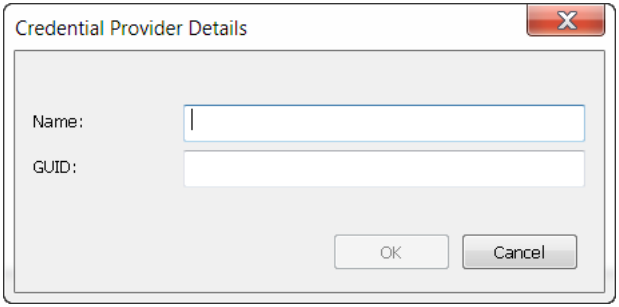
b Optional: Modify the text that appears on the self-service password reset link.

20 Click **Next**. The **Specify other allowed credential providers** page appears.



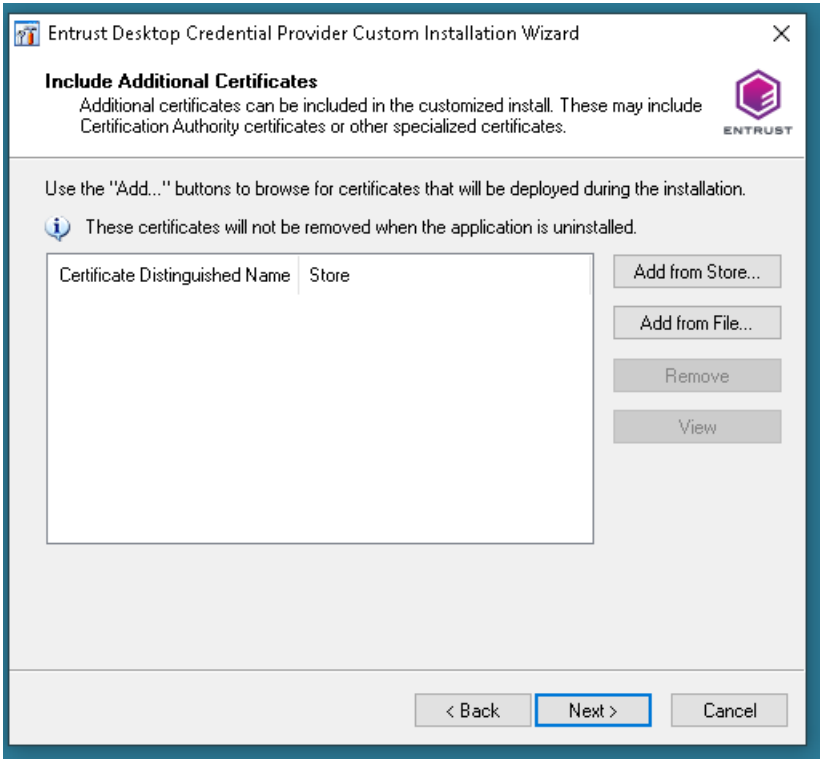
21 You can use this wizard to add other credential providers to Entrust Desktop, or you can add them from a `AllowCredentialProviders.ini` file, as described in "Adding certification providers from a file" on page 196. If you have already added other credential providers using the `AllowCredentialProviders.ini` 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



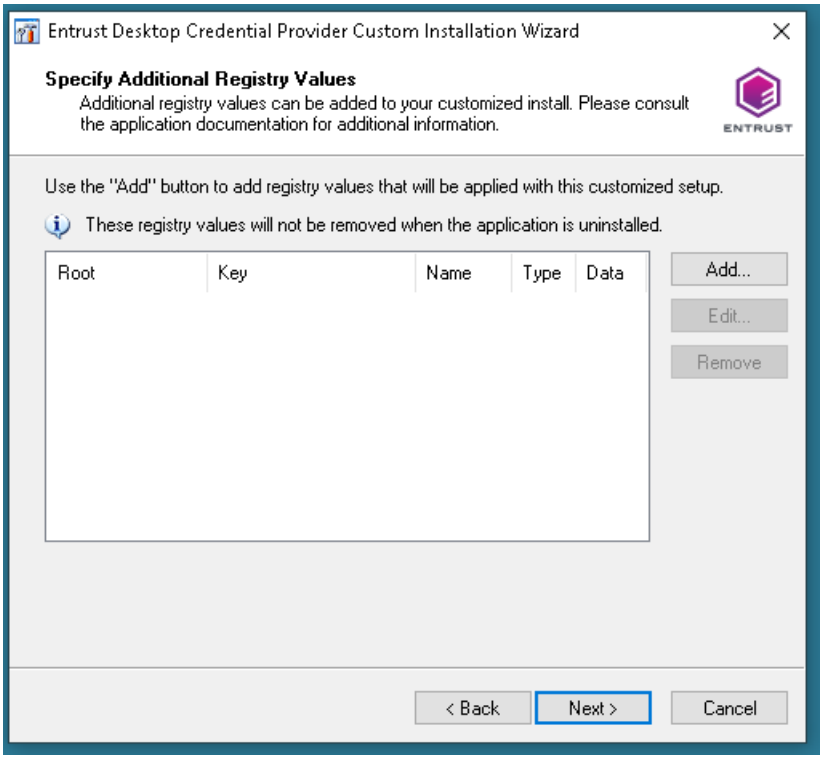
22 Enter the name of the credential provider and the globally unique identifier (GUID) for the credential provider, and then click **OK**.

The **Include Additional Certificates** page appears.



23 Click **Next** to skip this step as the trusted CA is in your root CA store.

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



24 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 199).

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**.

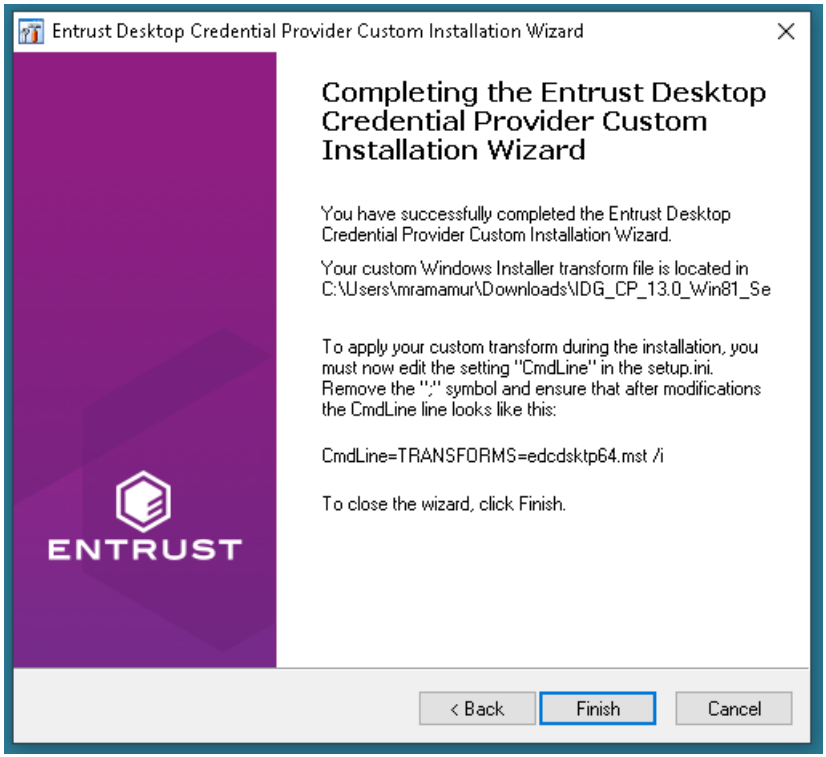
b After you have entered all your settings, click **OK**.

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 225.

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



25 Read the instructions for applying the custom transform file (`MST`) during the installation. See "Applying your custom transform file during installation" on page 92 for further instructions.

26 Click **Finish** to close the wizard and save the transform file.

27 Go to "Applying your custom transform file during installation" on page 92.

Installing for Entrust Identity Enterprise

Use this procedure to install Entrust Desktop for Windows for Entrust Identity Enterprise authentication.

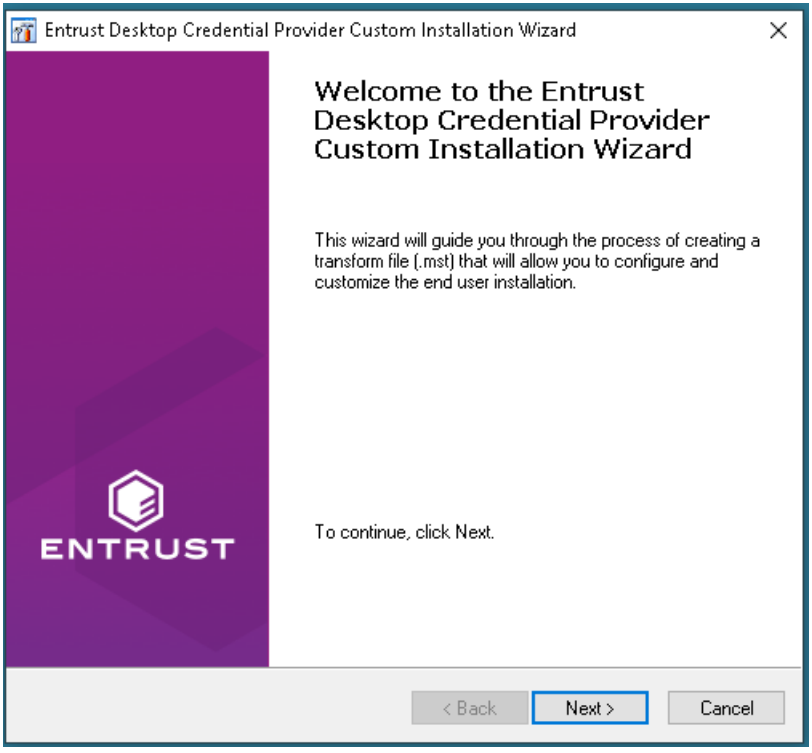
To install for Entrust Identity Enterprise

1 Launch the **Custom Installation** wizard as follows:

   a Navigate to the `<IDG_CP_13.0_extracted_folder>\Utilities\` folder.

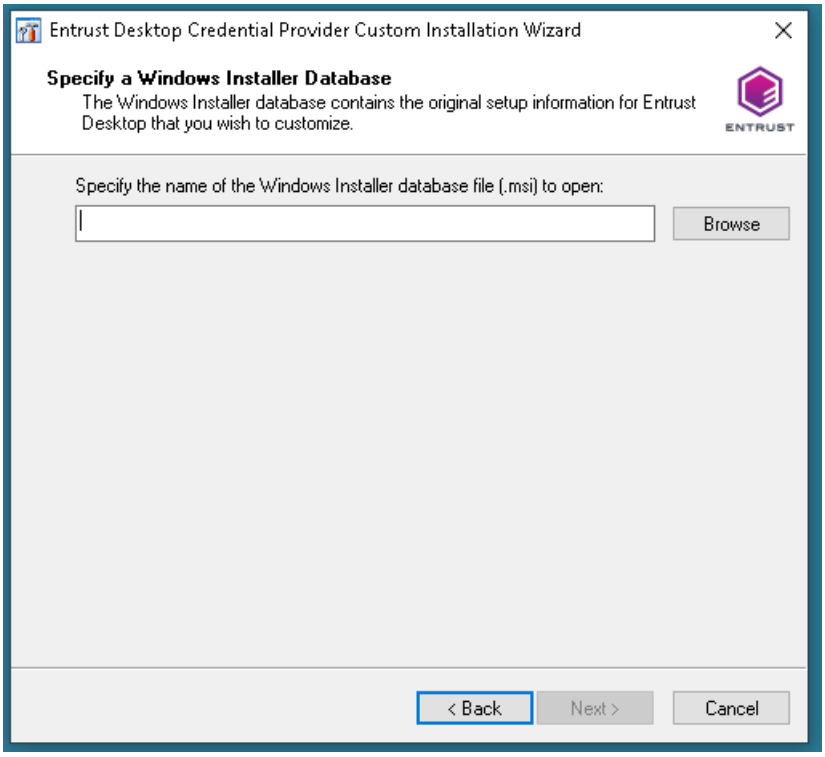
   b Double-click `edcwincustwiz64.exe`. (or `edcwincustwiz32.exe`).

   The **Entrust Desktop Setup** wizard appears.



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

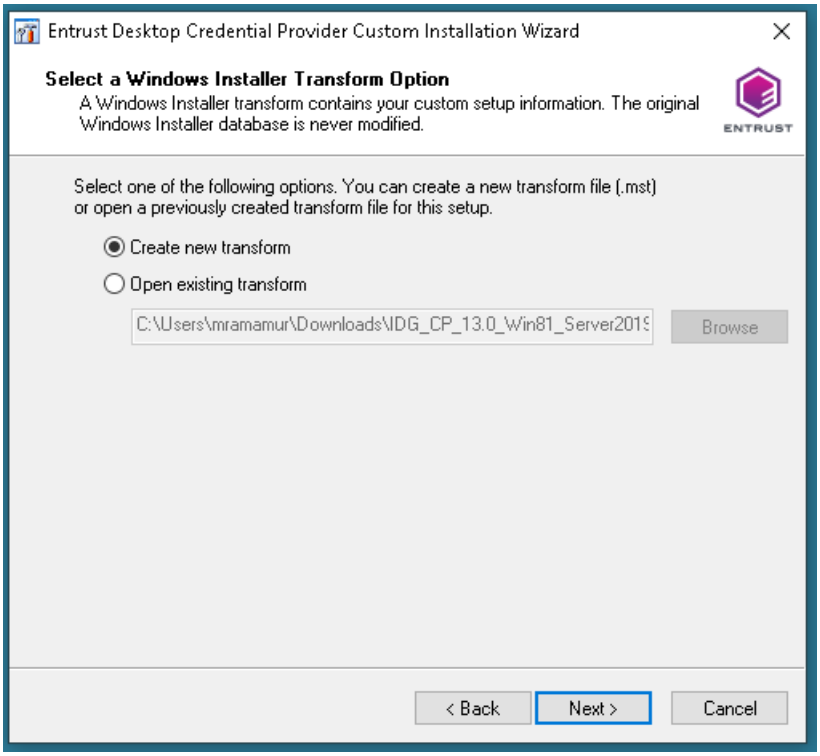
The **Specify a Windows Installer Database** page appears.



3 Enter the path for the Entrust Desktop for Microsoft Windows installation file (`edcdsktp64.msi` or `edcdsktp32.msi`). This file is included with your Entrust Desktop for Microsoft Windows software.

4 Click **Next**.

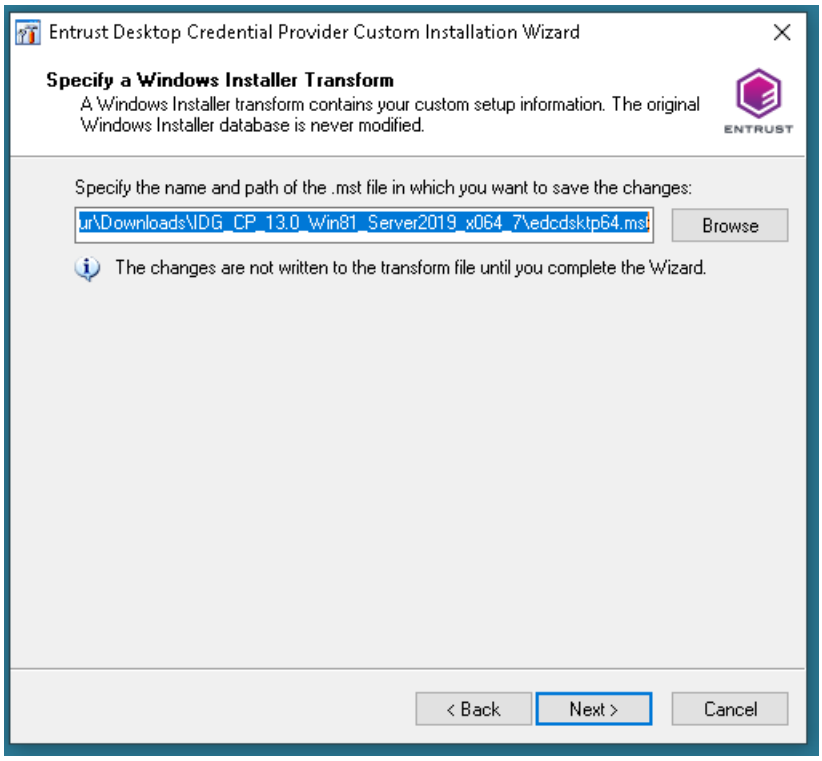
The **Select a Windows Installer Transform Option** page appears.



5 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.

6 Click **Next**.

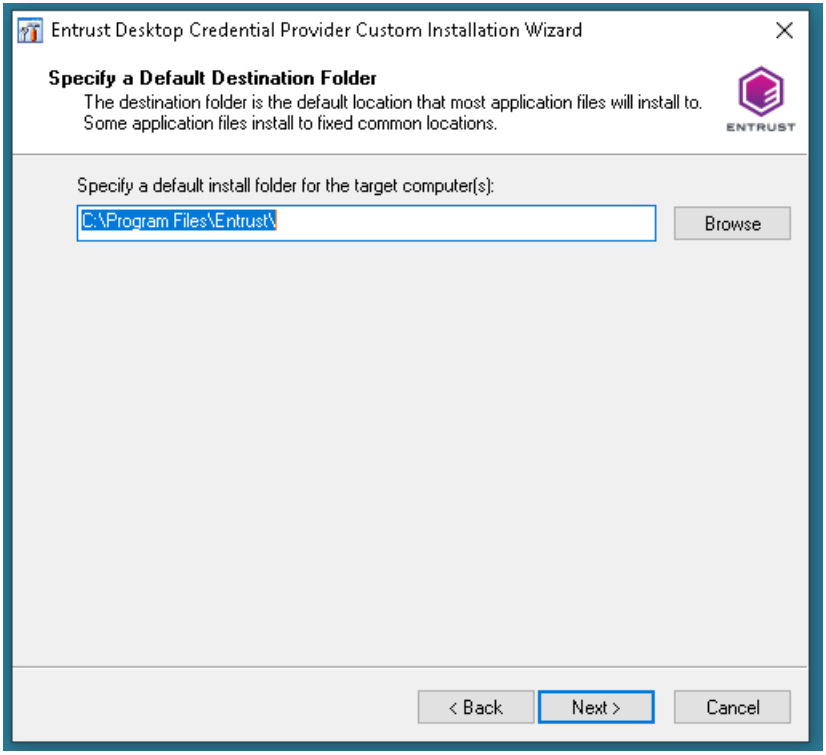
The **Specify a Windows Installer Transform** page appears.



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.

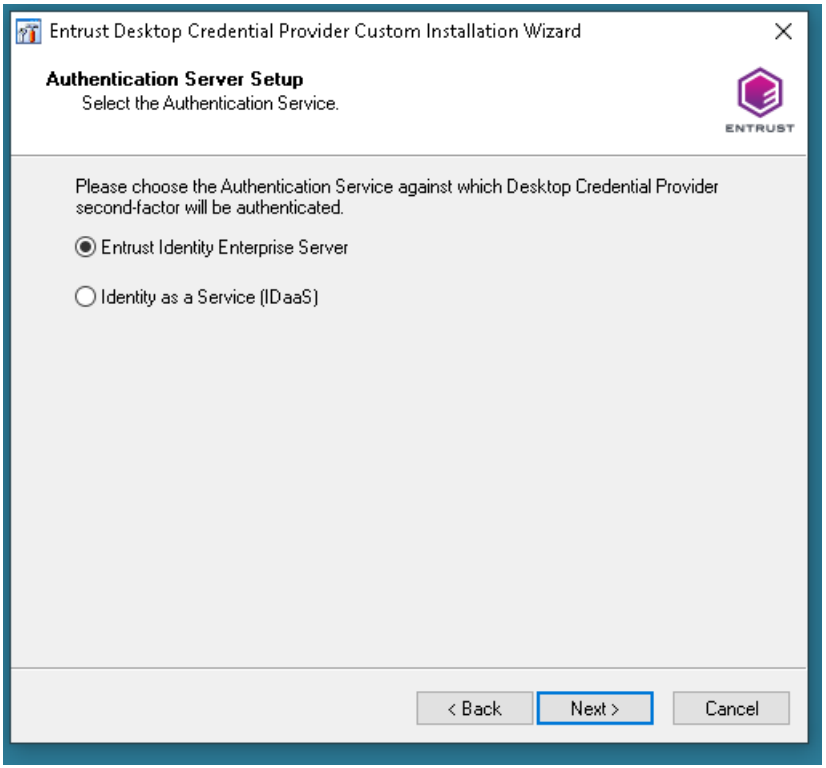
7 If you are creating a new transform file, specify the path and the file name. Browse to the `MST` file in which to save your custom setup information and click **Next**.

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



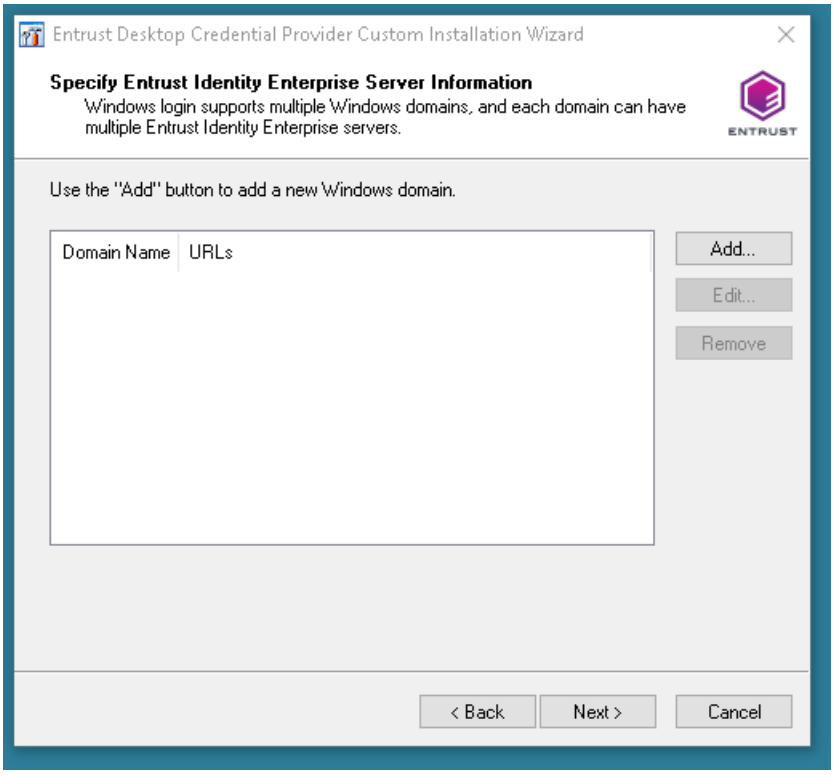
8 Select the default installation folder on the target computer and click **Next**.

The **Authentication Server Setup** page appears.



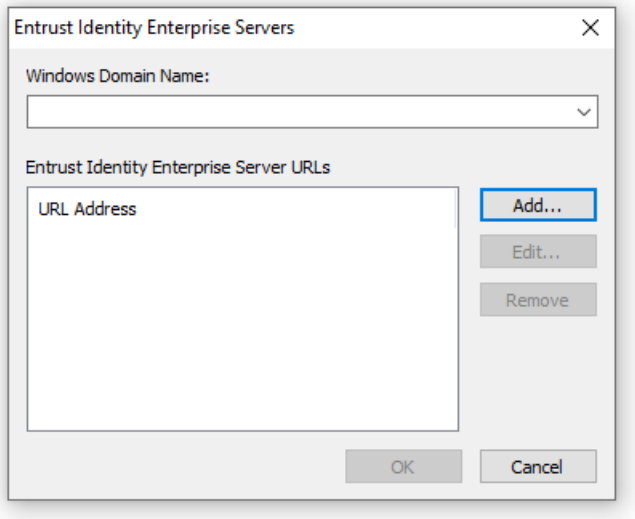
9 Select **Entrust Identity Enterprise Server** and then click **Next**.

The **Specify Entrust Identity Enterprise Server Information** page appears.



10 Set the **Entrust Identity Enterprise Servers** as follows:

a Click **Add** to add Windows domains and Entrust Identity Enterprise Server URLs.



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 Identity Enterprise is located. For a workgroup paired system, enter the localhost under the Windows Domain Name.

Note:
Domain names cannot contain spaces.

c On the **Entrust Identity Enterprise Servers** dialog box, click **Add**.

The **URL Address** page appears.

d Enter the Entrust Identity Enterprise 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/services/AuthenticationServiceV11
```

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

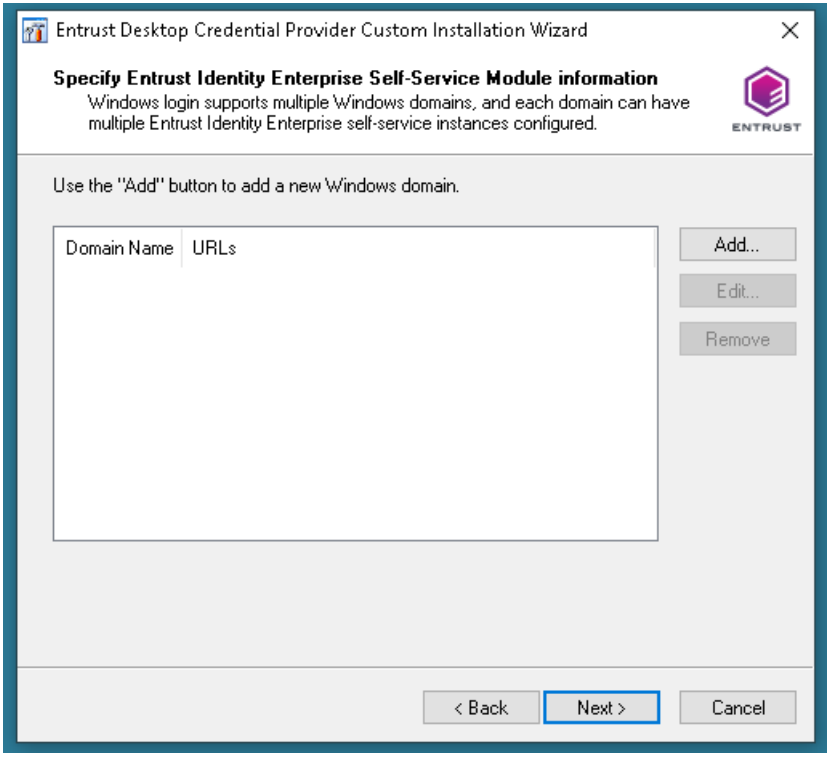
If you have more than one Entrust Identity Enterprise Server in your environment, repeat Step a to Step c to add URLs for those servers.

Entrust Desktop Client allows you to add multiple Entrust Identity Enterprise 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 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 Step a to Step e.

11 Click **Next** on the **Entrust Identity Enterprise Server Information** page.

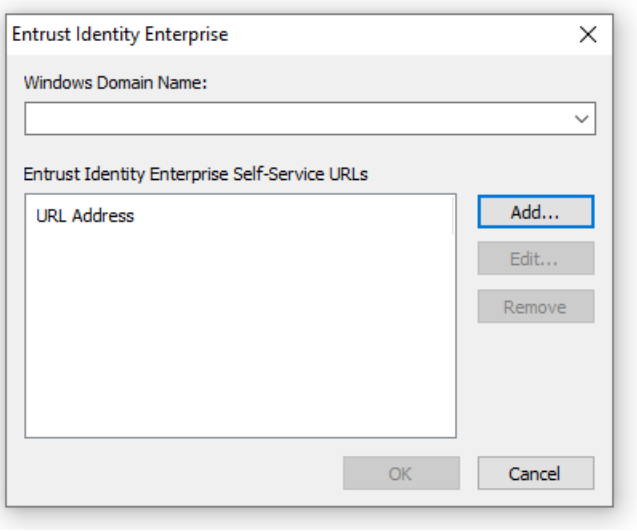
The **Entrust Identity Enterprise Self-Service Module information** page appears.



12 Set the Self-Service Server information as follows:

a Click **Add** to specify Self-Service Server information.

The **Entrust Identity Enterprise Self-Service** page appears.



b From the **Windows Domain Name** drop-down list, select the domain for which you want to configure Self-Service Module.

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.

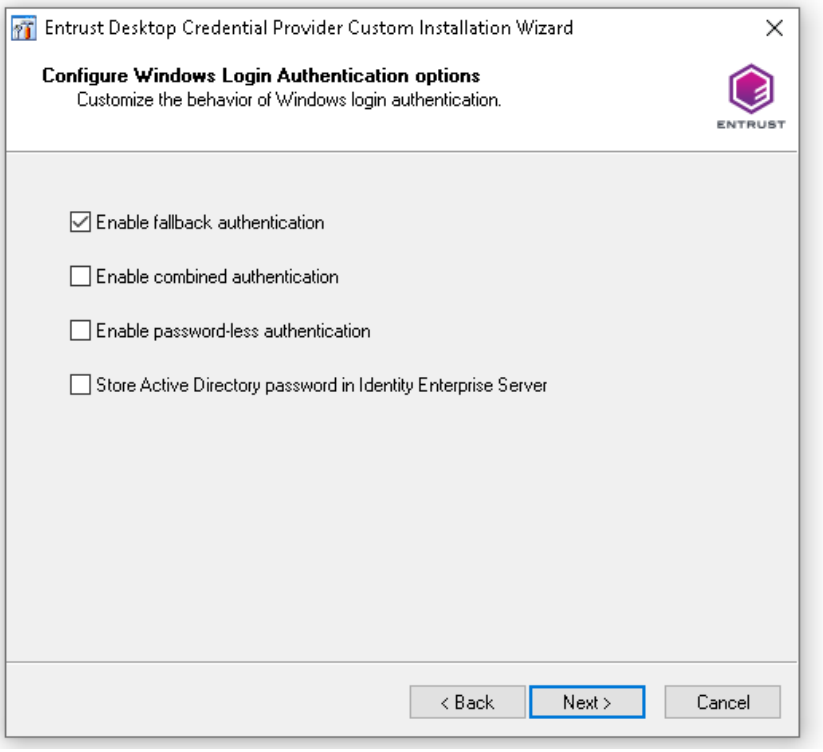
e Click **OK** to close the Entrust Identity Enterprise Self-Service dialog box.

If you have more than one Entrust Identity Enterprise Self-Service server in your environment, repeat Step a to Step d to add URLs for those servers.

Entrust Desktop Client allows you to add multiple Entrust Identity Enterprise Self-Service URLs. The URLs you enter in this step are stored sequentially in the registry, in the same order as they 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 Identity Enterprise Self-Service Module Information** page.

The **Configure password-less and offline Token authentication options** page appears.



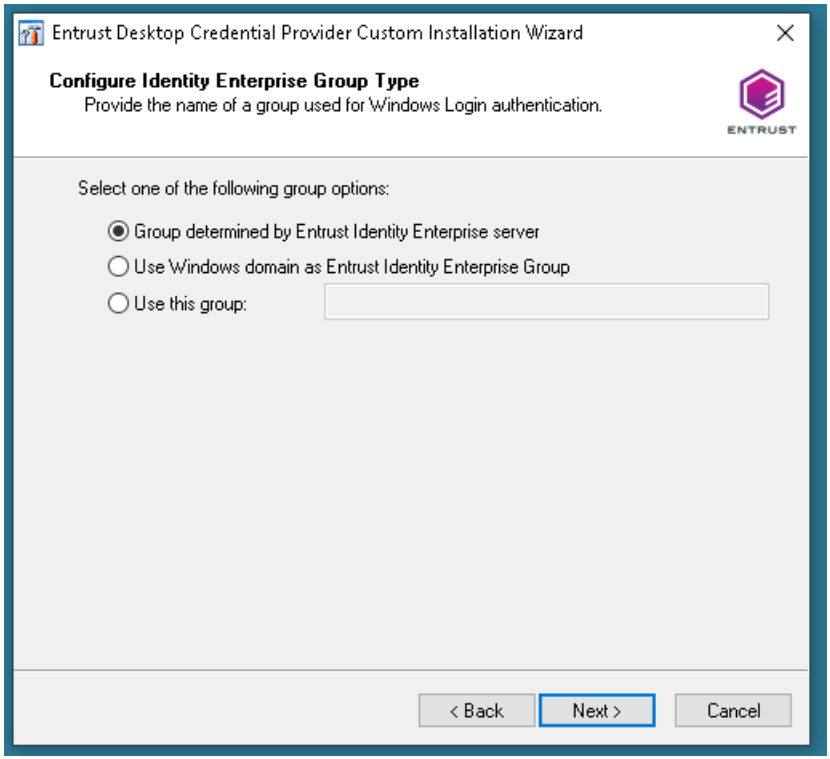
14 To specify the password-less, offline token, fallback authentication, and combined authentication options:

- **a** Select **Enable password-less authentication** and **Store Active Directory password in Entrust Identity Enterprise 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 Desktop for Windows allows offline token authentication. For more information on how offline token authentication works, see "How the offline token works" on page 162.
- **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 E**nable 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 Entrust Identity Enterprise Group Type** page appears.



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

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

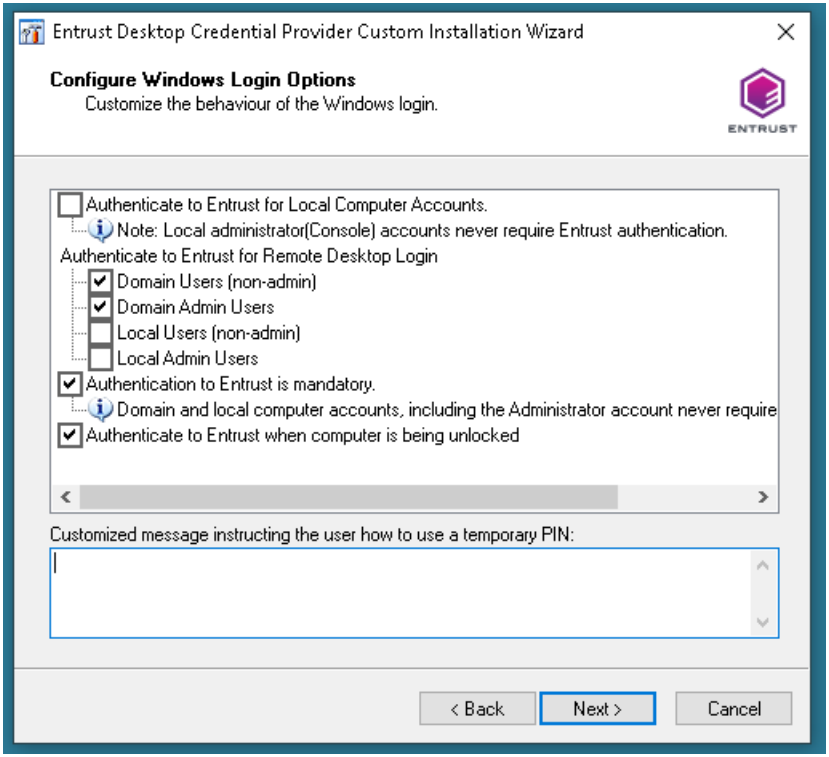
would create a package for all users in group A and a different package for all users in group B.

- To allow Entrust Identity Enterprise to set the group, select **Group determined by Entrust Identity Enterprise.**
- To use the Windows domain as the group, select Use Windows domain as **Entrust Identity Enterprise 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:

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

Note:
Local computer accounts, including the Administrator account, never require Entrust Identity Enterprise authentication.

b To require users to authenticate when unlocking their computers, select **Authenticate to Entrust when computer is being unlocked**. If you deselect this box, users that are not registered in Entrust Identity Enterprise will be able to log in without a second factor challenge.

c To enable users to log in to the computer offline using question and answer authentication, **Select Enable Q&A for offline authentication.**

d To enable users to authenticate to computer using Local Computer Accounts. **Select Authenticate to Entrust for Local Computer Accounts**.

Note:
Local administrator accounts never require Entrust authentication in console login session.

- To enable authentication to Remote Desktop Login session using Entrust, the users are separated in four groups.
  - Domain Users (non-admin)
  - Domain Admin users
  - Local Users (non-admin)
  - Local admin Users

Allow local users

To allow Local Users (non-admin) and Local admin Users:

- S**elect Authenticate to Entrust for Local Computer Accounts**.
- If the user does not **Select Authenticate to Entrust for Local Computer Accounts**, then the value for Local Users (non-admin) and Local admin Users are not set, even if the user enters the registry values never require Entrust authentication.

For Remote Desktop login session (for example, if using the `mstsc` tool):

- If S**elect Authenticate to Entrust for Local Computer Accounts is** checked, second-factor authentication is performed for that checked user group.
- If unchecked, second-factor authentication is not performed for that unchecked user group.

Entrust Desktop for Windows always validates user credentials irrespective of this option (checked or unchecked). This authentication is done to verify the user name and password.

For valid user credentials, Entrust Desktop for Windows creates an authentication package containing the user name and password and returns it to Windows, which performs its own authentication. This is done for all Remote Desktop login session or console logins and for domain and non-domain users (admin and non-admin).

This registry setting uses bit-flag, the combination of the above users are done in the following manner:

Users	Default Values for each user																
Domain User	1	0	1		1		1		1		1		1		1		1
Domain Admin	2	0		2	2			2	2			2	2			2	2
Local User	4	0				4	4	4	4					4	4	4	4
Local Admin	8	0								8	8	8	8	8	8	8	8
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Figure 3 shows all values of `AuthenticateRDPLogin` registry setting and whether the second factor screen appears for all or for specific user groups.

If the cell value is Yes, the second-factor authentication screen appears for remote desktop (RDP) client login session.

If the cell value is No, he second-factor authentication screen does not appear for remote desktop (RDP) client login.

Figure 3: "AuthenticateRDPLogin" registry setting for RDP users

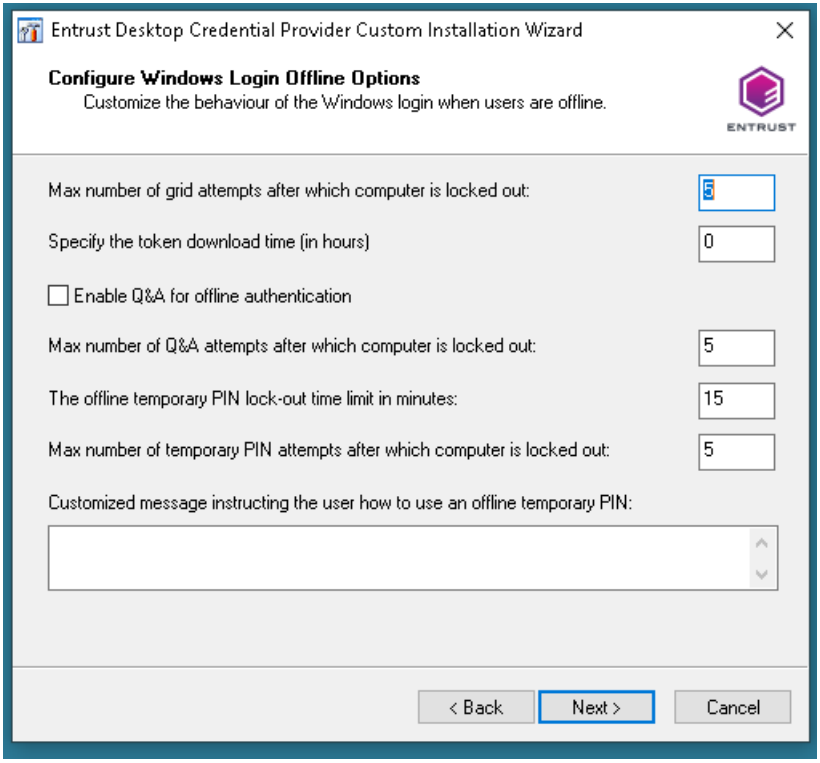
	Domain User		Local User	
Value	No-Admin	Admin	Non-Admin	Admin
0	No	No	No	No
1	Yes	No	No	No
2	No	Yes	No	No
3	Yes	Yes	No	No
4	No	No	Yes	No
5	Yes	No	Yes	No
6	No	Yes	Yes	No
7	Yes	Yes	Yes	No
8	No	No	No	Yes
9	Yes	No	No	Yes
10	No	Yes	No	Yes
11	Yes	Yes	No	Yes
12	No	No	Yes	Yes
13	Yes	No	Yes	Yes
14	No	Yes	Yes	Yes
15	Yes	Yes	Yes	Yes

- 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.



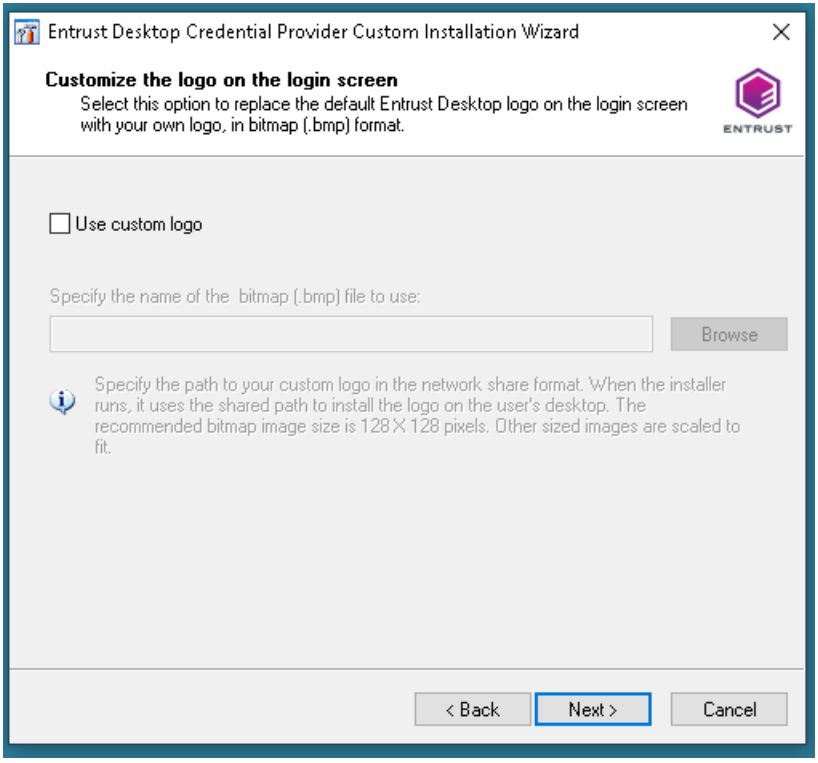
Note:
Add custom messages if your users need special instructions, or instructions in another language.

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.



This logo appears in the CredUI login screen. In addition, Entrust Desktop displays the selected Logo for **Other User** tile in a non-domain joined PC.

22 If you want to replace the default Entrust Identity Enterprise 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.

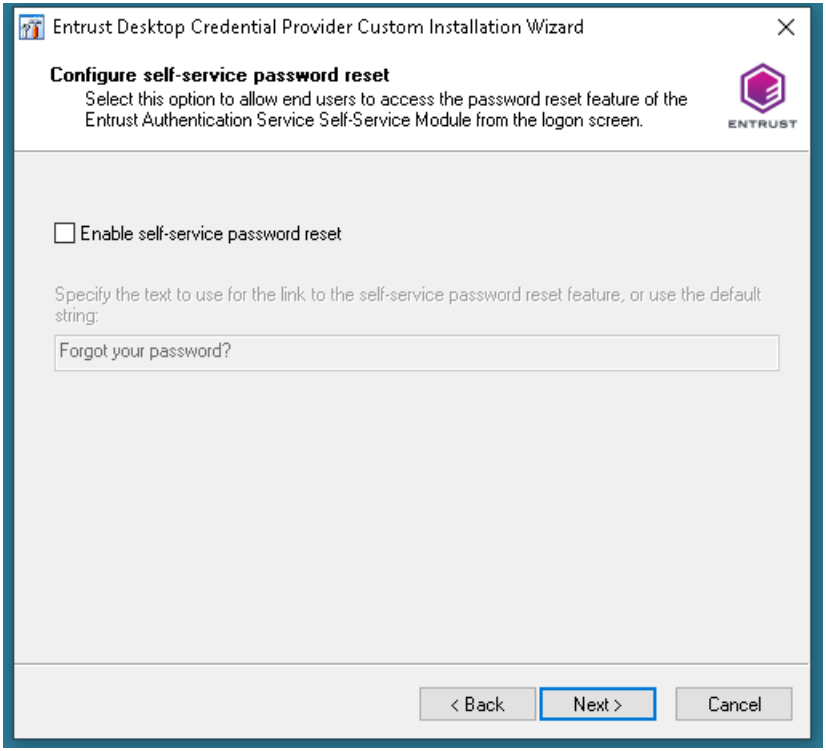
The image must be located in a network share accessible to users when they install the desktop client. The path must be in the following format:
`\\<path>\<image_file>.bmp`

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.

Note:
Custom logo appears only for CRED-UI and local user logins.

23 Click **Next**.

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



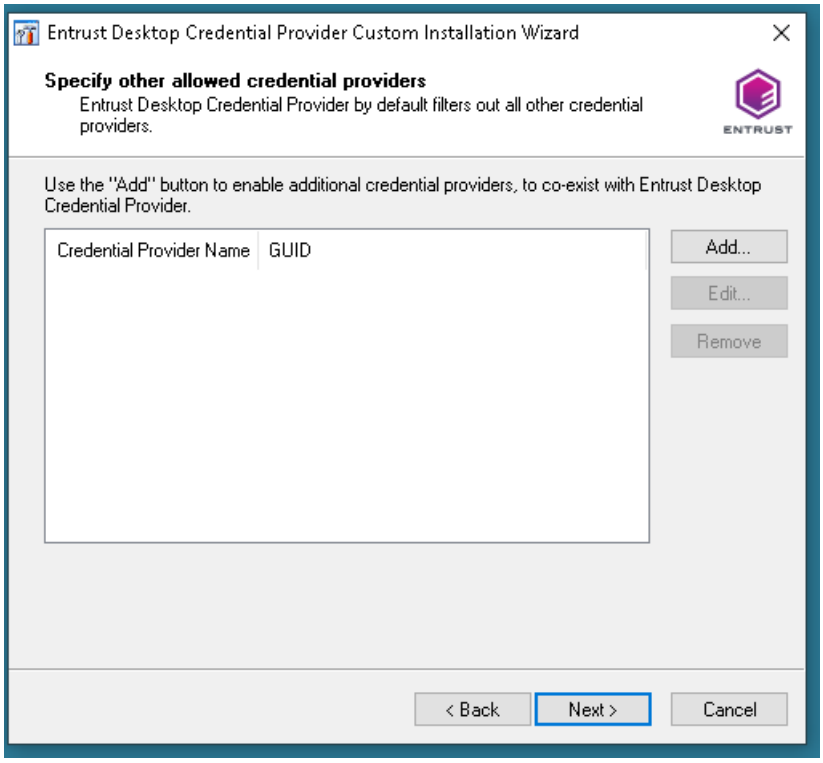
24 If you want users to be able to access the Entrust Identity Enterprise Self-Service Module (SSM) to reset forgotten passwords, select **Enable self-service password reset**. When this option is selected, a link to SSM appears on each user's login page.

Note:
For important information on using this feature, see "Desktop client and SSM integration overview" on page 230.

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 40).

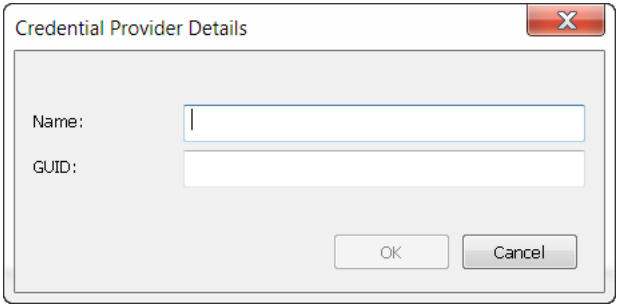
25 If you want to customize the text of the link the SSM, enter a new text in the text box. Otherwise, the default text is used.

26 Click **Next**. The **Specify other allowed credential providers** page appears.



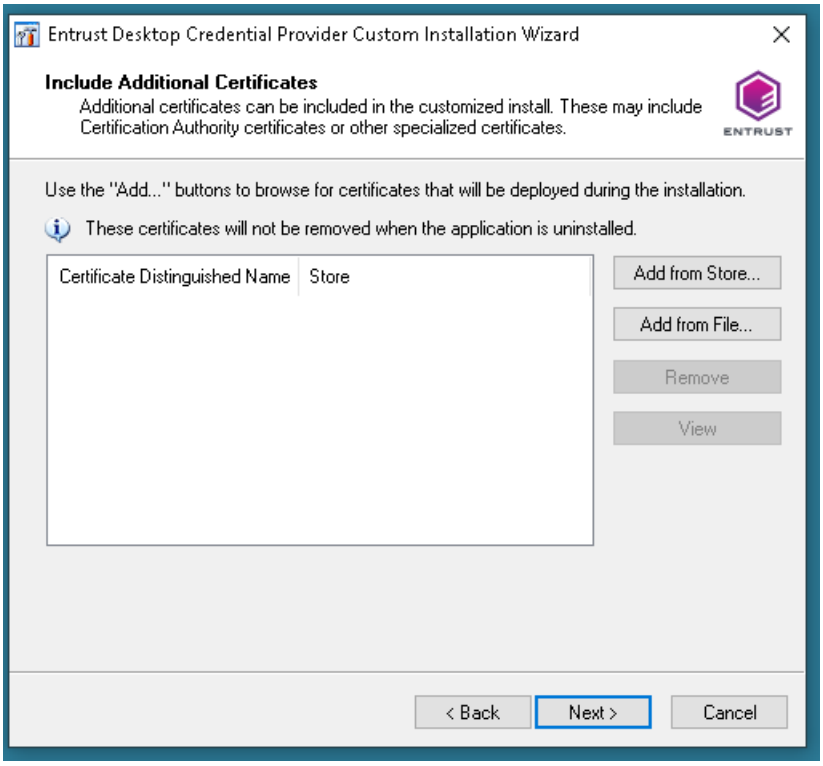
27 You can use this wizard to add other credential providers to Entrust Desktop, or you can add them from a `AllowCredentialProviders.ini` file, as described in "Adding certification providers from a file" on page 196. If you have already added other credential providers using the `AllowCredentialProviders.ini` 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



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.



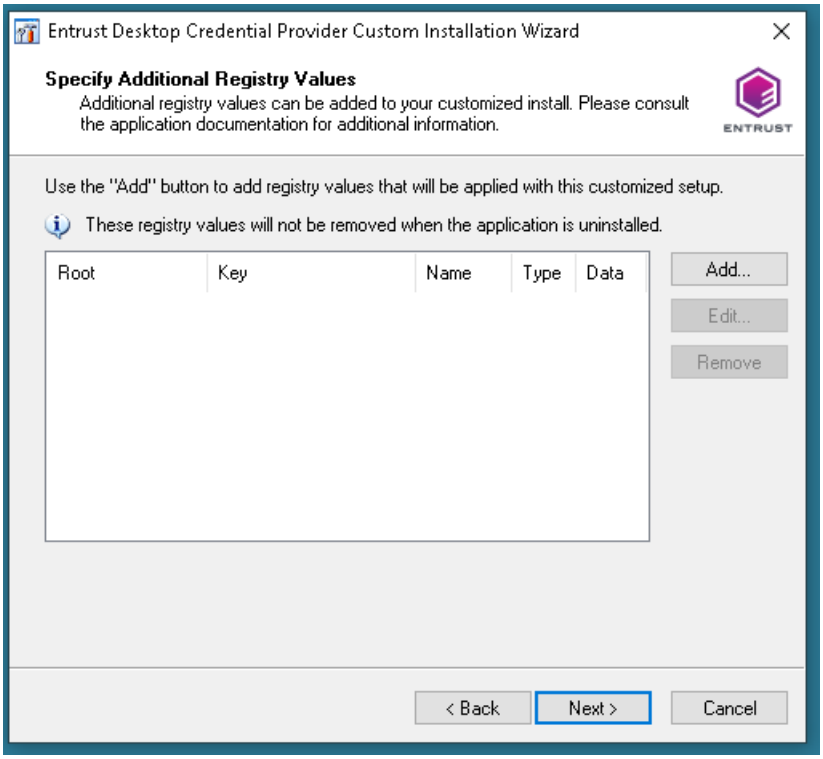
29 If installing for **Entrust Identity Enterprise Server**, add the certificate from the Entrust Identity Enterprise described in the section "Communication between Desktop for Microsoft Windows and the Entrust Identity Enterprise" and any other certificates that may be required for secure communication.

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 199).

Note:
If you selected the **Enable self-service password reset**, see more information in "Desktop client and SSM integration overview" on page 230.

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**.

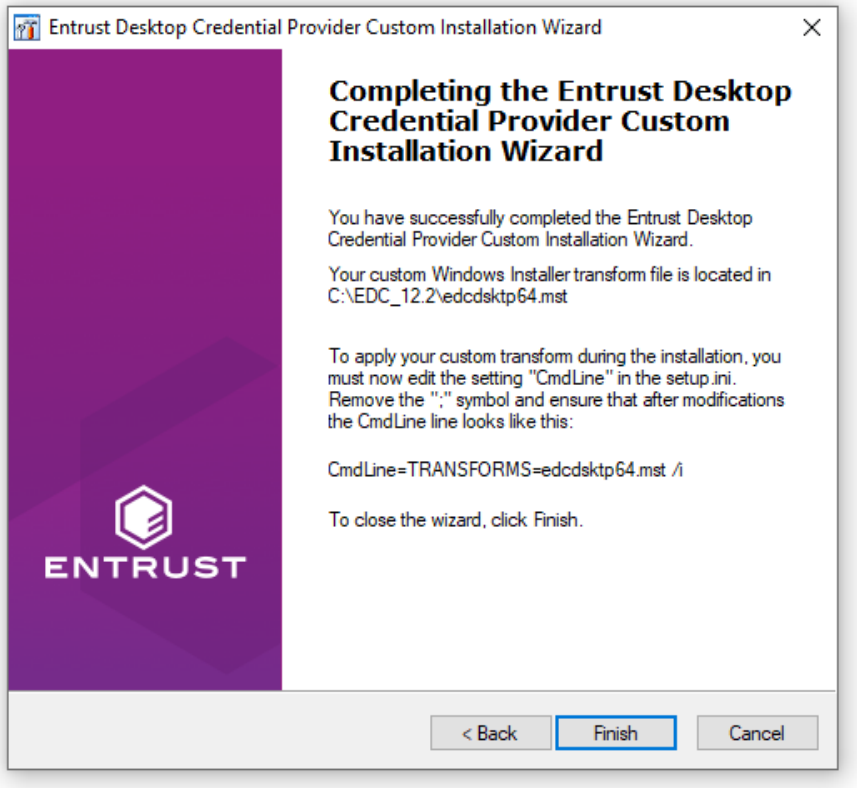
b After you have entered all your settings, click **OK**.

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 225.

The **Completing the Entrust 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 92 for further instructions.

33 Click **Finish** to close the wizard and save the transform file.

34 Proceed to “Applying your custom transform file during installation” on page 92.

Applying your custom transform file during installation

When you finish creating your custom transform (MST) file using the **Entrust Desktop Credential Provider 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 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 "edcdsktp64.mst" with the name of the
transform you want to apply.

;CmdLine=TRANSFORMS=edcdsktp64.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 edcdsktp64.mst, the setup.ini will look like this:

```
;To apply a transform, please remove the ";" symbol in the
following line and replace "edcdsktp64.mst" with the name of the
transform you want to apply.

CmdLine=TRANSFORMS=edcdsktp64.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 Desktop for Microsoft Windows Installer package (`edcdsktp64.msi or edcdsktp32.msi)` and the installation begins.

Note:
If you want users to install the software by running the `setup.exe`, you must also copy the `edcdsktp64.msi (or edcdsktp32.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 94 for further information about making the installation files available to users.

Distributing the installation package

By running the **Custom Installation** wizard (`edcwincustwiz64.exe` or `edcwincustwiz32.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 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 94
- "Making the installation package available on the Web" on page 95
- "Using third-party software distribution tools" on page 96
- "Performing a silent installation" on page 96

Making the installation package available on the network

You can run the Windows Installer file (`edcdsktp64.msi or edcdsktp32.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 (`edcdsktp64.msi or edcdsktp32.msi`), which contains Entrust 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 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 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 92 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 96 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>/edcdsktp64.msi (or edcdsktp32.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>/edcdsktp64.msi
TRANSFORMS=http://<path_to_files>/edcdsktp64.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 "edcdsktp64.mst" with the name of the
transform you want to apply.
;CmdLine=TRANSFORMS=edcdsktp64.mst /i
```

2 Remove the semicolon (;), and replace

```
CmdLine=TRANSFORMS=edcdsktp64.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 97 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 **Cancel** 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 **Cancel** 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 **Cancel** 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 **Fatal Error**, **User Exit**, or **Exit** modal dialog boxes at the end of the installation.

Creating an administrative installation

Typically, administrators deploy Entrust 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://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 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 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 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 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:\edcdsktp64.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 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\edcdsktp64.msi" TRANSFORMS="\\nwksvr\IG\edcdsktp64.mst"
```

Example of a URL path:

```
msiexec /i "http://svr/edcdsktp64.msi" TRANSFORMS="http://svr/edcdsktp64.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 101.
- 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 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 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\edcdsktp64.msi" REINSTALL=ALL REINSTALLMODE=vomus
```

Example of a URL path:

```
msiexec /i "http://svr/edcdsktp64.msi" REINSTALL=ALL REINSTALLMODE=vomus
```

Note:
Do not use relative paths.

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

c 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 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 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 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 edcdsktp64.msi TRANSFORMS=edcdsktp64.mst /qn
```

Example for a 32-bit installation:

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

```
msiexec.exe /i edcdsktp32.msi TRANSFORMS=edcdsktp32.mst /qn
```

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

The second line installs the new version of Entrust 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>\edcdsktp64.msi REMOVEWIGLOFFLINEKEY=0
```

for a 32-bit installation:

```
msiexec /x <path>\edcdsktp32.msi REMOVEWIGLOFFLINEKEY=0
```

where:

`<path>` is the path to the `edcdsktp32.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.

3

How Entrust Desktop for Windows works

This chapter describes user interaction with Entrust Desktop for Windows for authentication:

Authentication with Entrust 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

After entering their Windows user name and password, the 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 to authenticate to Entrust Identity Enterprise or Identity as a Service.

If the user's response is correct, the user is able to access their desktop. Whether the desktop is accessible to users without Entrust Identity Enterprise or Identity as a Service authentication set up is configurable when the Entrust Identity Enterprise or Identity as a Service installation package is created. See "Create a custom installation package" on page 50 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 Identity Enterprise or Identity as a Service. See the *Entrust Identity Enterprise Administration Guide* or the *Identity as a Service Administration Online Help* for further information.

If an Entrust user is online and clicks **Use Temporary PIN**, Entrust 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 "Create a custom installation package" on page 50 for more information about customizing this message.

Authentication with Identity as a Service

The Desktop Application can connect to the Identity as a Service and perform second factor authentication.

Entrust Desktop for Microsoft Windows supports the following Identity as a Service Authenticators:

- Entrust Soft Token Push
- Software/Hardware token
- Grid card
- Voice/SMS/Email One-time password
- Knowledge-based authenticator
- Smart Credential
- Temporary Access Code
- Passkey/FIDO2
- Face Biometric

Offline challenges

Entrust Desktop for Windows can use strong second-factor authentication to log in users, even if they are temporarily out of contact with the Entrust Identity Enterprise or Identity as a Service. 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.

After installing Entrust Desktop for Windows, a user can sign in to a computer that is disconnected from the corporate domain—without first signing in while it is connected. The user must have signed in to that computer at least once before installing Entrust Desktop for Microsoft Windows.

The following types of challenges can be used offline:

- “Offline grid challenges”
- “Offline token challenges”
- Offline Q&A (question and answer)
- Offline temporary PIN

Offline grid challenges

When a user authenticates using GRID on the second-factor page, only offline Grid is stored in the registry for the user, and the offline token is not downloaded in this case.

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 user must also use Ao1 to log in offline. A01 will not be accepted. Offline responses are also case sensitive.

Note:
The policy configured on the Entrust Identity Enterprise 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 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 Identity Enterprise or Identity as a Service and the Windows registry setting for offline token login (see "Registry settings under 'WIGL'" on page 201). 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 Identity Enterprise must allow for offline token challenge with or without PVN. PVN is not supported with Identity as a Service.

In the **Minor hours** setting, set the amount of time, in hours, that Entrust Identity Enterprise or Identity as a Service will allow offline validation by OTP. In the **Max hours** setting, set the maximum amount of time, in hours, that Entrust Identity Enterprise or Identity as a Service 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`.

Migrating users from Entrust Identity Enterprise to Identity as a Service

This section explains how to migrate users from Entrust Identity Enterprise to Identity as a Service and then how to authenticate them from Entrust Desktop for Windows after migration.

Prerequisites

Before beginning the migration process, verify the following:

1. Ensure that users exist in Entrust Identity Enterprise with one of the following assigned authenticators:
   - Grid
   - One-time password (OTP)
   - Token
   - Knowledge-based authentication (KBA
2. Verify the list of users in a group that will be exported from Entrust Identity Enterprise and imported into Identity as a Service.
3. Verify end-to-end use cases with Entrust Desktop for Windows against Entrust Identity Enterprise.

Note:
For instructions on how to find users accounts, including groups and assigned authenticators in Entrust Identity Enterprise, see the *Entrust Identity Enterprise Server 13.0 Server Administration Guide* available on Entrust TrustedCare.

To migrate users to Identity as a Service

1. Export the user list from Entrust Identity Enterprise, as follows:
   a. Open Master User Shell in an Entrust Identity Enterprise Virtual Machine.
   b. At the command prompt (if running Entrust Identity Enterprise release 12.x or 13.x), enter the following:

      ```
      system authexport -file <filename> -group <groupname>
      ```

      where `-file` <filename> is the file to which the data is exported. This argument is required.

      For example:

      ```
      system authexport -file IDGGroupData -group VPN
      ```

The status shows that the export completed successfully.

2. Obtain the strong password that Entrust Identity Enterprise or Migration Tool 3.0 created internally to encrypt the exported data file, as follows:

   a. Log in to Master User Shell or Migration Tool 3.0 using the following command:

      ```
      system authexport -password
      ```

   b. Make note of this password. The password is required to import the exported data into Entrust Identity as a Service.

3. Import the exported user list from Entrust Identity Enterprise in to Identity as a Service using the bulk operation to Migrate Users to in Identity as a Service. See the section, Migrate Entrust Identity Enterprise users to IDaaS in the Identity as a Service Administrator Help. Use the password noted in Step b above.

4. Reconfigure Entrust Desktop for Windows to use Identity as a Service for authentication, as follows (see Table 4 on page 112):

   a. Navigate to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL`.

   b. Set the registry key `UseIntellitrustServer` to `1`.

   c. Create a Key under WIGL and name it `IDaaS`.

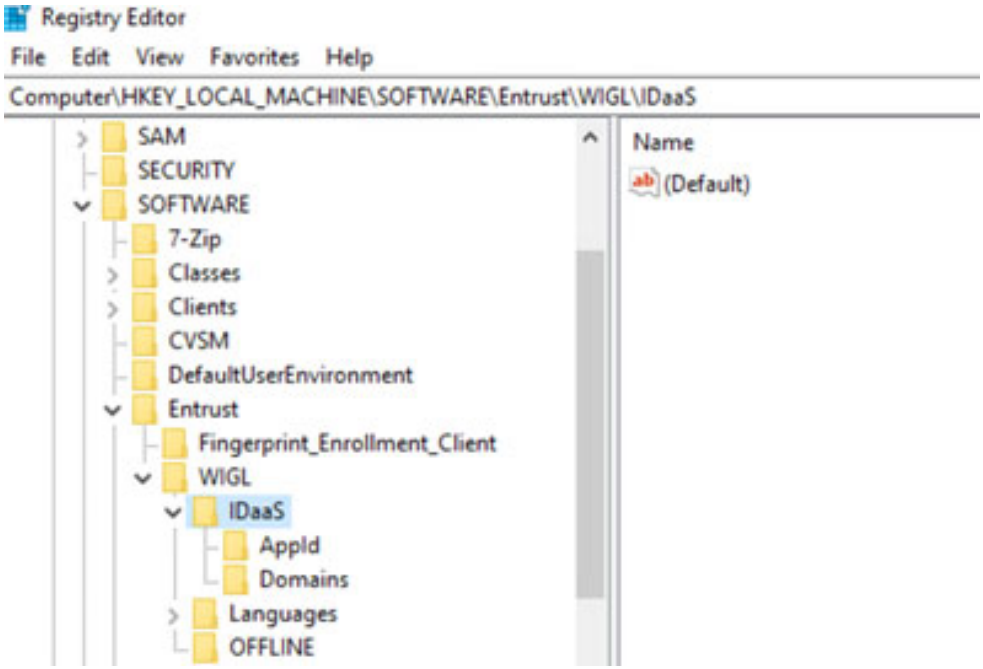
   d. Create Key under `IDaaS` and name as `AppId`.

   e. Create a String Value under `AppId` and provide domain name and `AppId` value.

   f. Create a Key under `IDaaS` and name it `Domains`.

   g. Create a String Value under `Domains` and add a domain name and IDaaS URL.

Figure 4: Reconfigure Entrust Desktop for Windows to use IDaaS



The user authentication process

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

Note:
Screenshots shown are provided as examples and reflect login with Entrust Identity Enterprise.

First-factor authentication

How it works

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

Entrust Desktop for Windows users begin logging into the domain by entering their user name and their Windows password. Entrust 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 protecting the domain. Unregistered users may be treated differently (see "Users without Entrust" on page 174).

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.

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.

Entrust Desktop options in the first-factor page

Entrust Desktop options groups less frequently used feature links in order to make more room for on login screen.

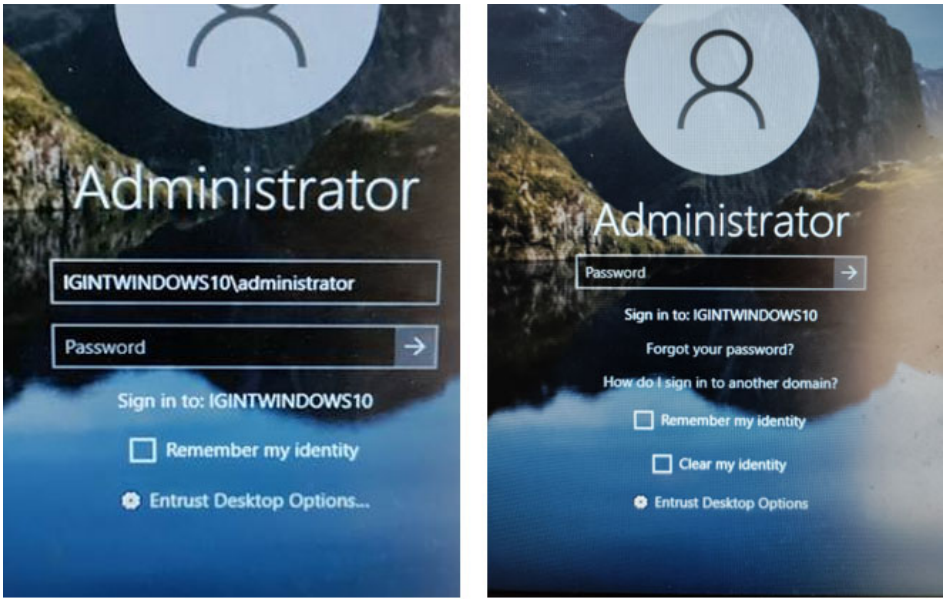
The user needs to click **Entrust Desktop Options** on the first-factor page to view the options.

How do I sign in to another domain? is the default Entrust Desktop Option.

When `EnablePwdReset` and `EnableRBAAuth` are set, the Entrust Desktop options include:

- Forgot your password? (See "Installing for Identity as a Service" on page 51).
- How do I sign in to another domain?
- Clear my Identity (See "How RBA works" on page 144 for more information).

Figure 5: Entrust options on the first-factor screen



Face Biometric with IDaaS

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

This procedure assumes that you have already integrated Entrust Desktop for Microsoft Windows with IDaaS. See Integrate Desktop for Windows with IDaaS in the *IDaaS Technical Integration Guides*.

To configure Entrust Desktop for Microsoft Windows with Face Biometric authenticator of IDaaS

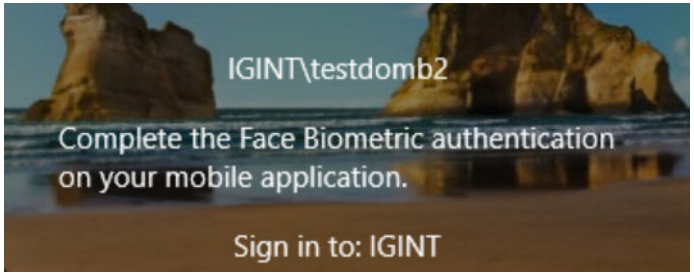
1. Configure Face Biometric for multifactor authentication. See Manage Face Biometrics by Onfido section in the *IDaaS Administrator Help*.
2. Create a custom user login Authentication Flow to enable Face Biometric for second-factor authentication. See Create authentication flows in the *IDaaS Administrator Help*.
3. Create a resource rule that includes the Authentication Flow that enables Face Biometric for second-factor authentication. See Create a resource rule in the *IDaaS Administrator help*.

Note:
Entrust Desktop for Microsoft Windows supports Face Biometric authentication only.

Authenticate using Face Biometric

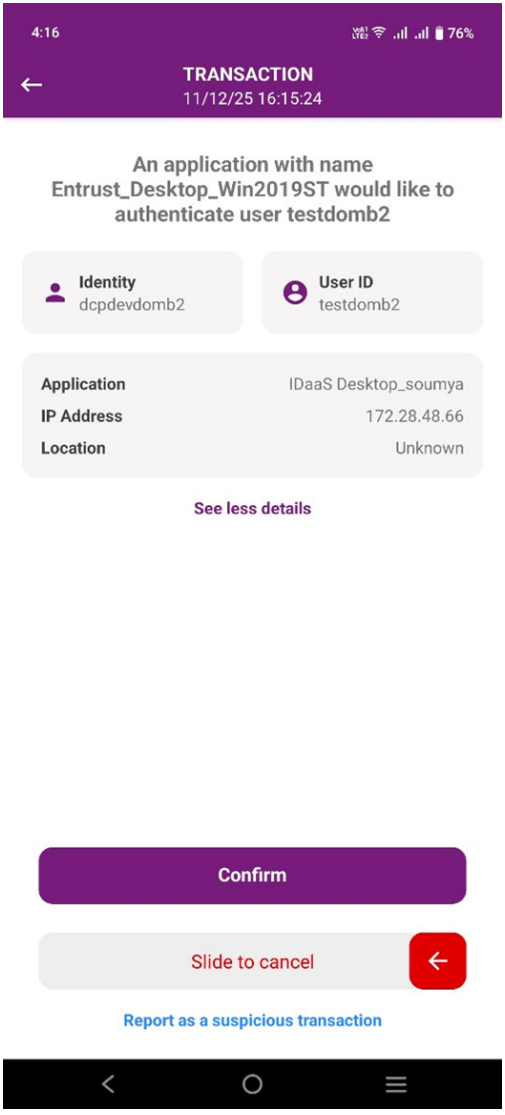
To authenticate using Face Biometric

1 Access the Entrust Desktop for Microsoft Windows resource and enter your username and password. The second-factor page appears prompting the user to complete Face Biometric authentication.



2 The user receives a notification on their mobile device in the Entrust Identity app.

3 The user clicks **Confirm** on the Entrust Identity app.



4 The user needs to scan their face and proceed with face recording.

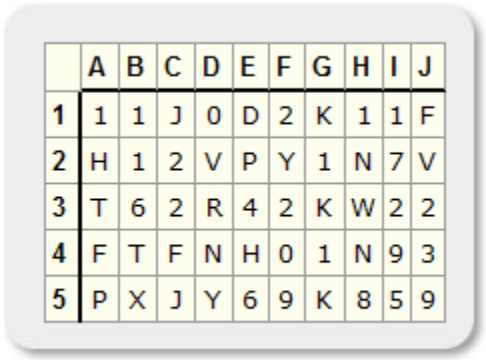
5 On successful authentication the user is redirected to the resource page.

Grid authentication

Users with grid authentication should be provided with an Entrust 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 167.

Authentication works as follows:

1. The user completes first-factor authentication successfully.
2. Entrust 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 validates the entered values and authenticates the user.
4. If you have required your Entrust 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.

Passkey/FIDO2 registration and authentication with Identity as a Service

Windows login supports Passkey/FIDO2 registration for second- factor authentication using physical USB keys (YubiKey) with Identity as a Service.

Passkey/FIDO2 authentication is supported for the following:

- Second-factor authentication for RDP, CREDUI, and the Windows console login.
- Password reset to reset the password.
- Registration for RDP, CREDUI, and Windows console login.
- Passkey/FIDO2 tokens registered in the IDaaS User portal can be used in Entrust Desktop for Windows.
- Passkey/FIDO2 tokens registered in Entrust Desktop for Windows can be used the IDaaS User portal.

Attention:
To configure Passkey/FIDO2 you need to refer to the Identity as a Service Administrator Help.

Configure FIDO2/Passkey registration and authentication

Complete the following to configure FIDO2/Passkey registration and authentication:

- “Configure FIDO2/Passkey authentication policies” on page 119
- “Configure an application for Passkey/FIDO2 authentication” on page 121
- “How does Passkey/FIDO2 authentication flow work with Identity as a Service?” on page 122
- “Reset a Passkey/FIDO2 Yubikey” on page 126

Configure FIDO2/Passkey authentication policies

You configure these settings in Identity as a Service. To complete this procedure you need to log in to your IDaaS Administrator account and refer to the Identity as a Service Administrator Help for specific instructions.

To open the help

1 Log in to Identity as a Service.

2 If the hyperlink provided does not work, access the *Administrator Help* by clicking the three dots next to your profile name and select **Help > Administrator Help**. The *Administrator Help* opens in another window.

To configure an application for Passkey/FIDO2 authentication

Before you begin, go to Manage Passkey/FIDO2 authenticators in the *Identity as a Service Administrator Help*).

1 Log in to Identity as a Service as an administrator.

2 Go to **Home > Policies > Authenticators > Passkey/FIDO2** to display the **Passkey/FIDO2** page.

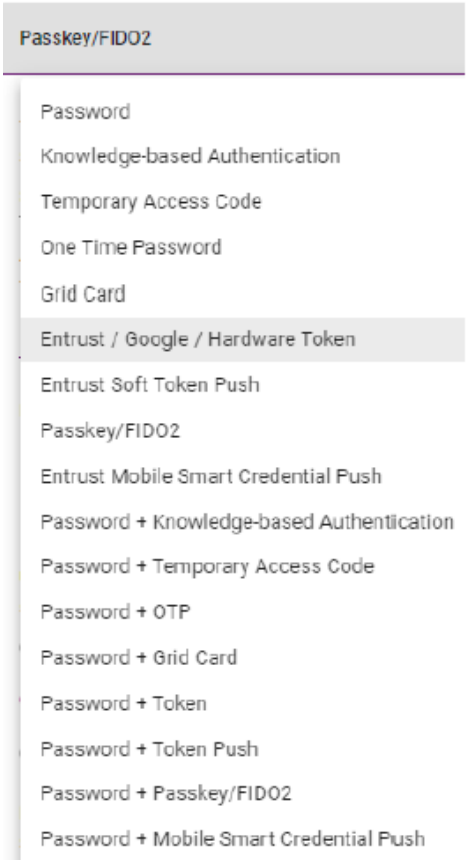
3 In the **Passkey/FIDO** page, set the following:

   a Select the **API minimum authentication level** from the drop-down list.

   When you select this setting, a drop-down list appears. The selected authenticator and any of the authenticators below it will work for Registration with Entrust Desktop for Windows.

   For example, if you select **Entrust / Google / Hardware Token** in the list, then **Entrust / Google / Hardware Token** and all authenticators listed below it will work for registration.

In this example, any of the authenticators listed above **Entrust / Google /Hardware Token** cannot be used for registration.



b For **User Verification**, select either **Required** or **Preferred**.

c For **Resident Key (User ID stored)** select either **Required** or **Preferred**.

d For **Authenticator Attachment**, select **Either** or **Cross-Platform**.

e Optional. Select **Enable Passkey/FIDO2 allowlist**.

f Click **Save**.

Configure an application for Passkey/FIDO2 authentication

You configure these settings in Identity as a Service. To complete this procedure you need to log in to your IDaaS Administrator account and open the Administrator Help.

To configure an application for Passkey/FIDO2 authentication

1. Log in to Identity as a Service as an administrator.
2. Create an IDaaS Authentication API and set the **Source of Client IP address for risk conditions** to **Provided in the API**. Leave the other settings at the default values.

   For more information, see the section, Integrate Authentication API in the I*dentity as a Service Administrator Help*.
3. Create a custom authentication flow with **External Authentication** for first-factor and **Passkey/FIDO2** for second-factor authentication.

   See Create authentication flows in the *Identity as a Service Administrator Online Help*.
4. Using the authentication flow, create a resource rule to protect Entrust Desktop for Windows for FIDO2/Passkey authentication with IDaaS.

   See Create IDaaS applications resource rules in the *Identity as a Service Administrator Guide*.

How does Passkey/FIDO2 authentication flow work with Identity as a Service?

Passkey/FIDO2 authentication uses public-key cryptography (generation and use of private and public keys) to validate a user's identity. Entrust Desktop for Windows uses the following flows for Passkey/FIDO2 authentication:

- Registration flow
- “Passkey/FIDO2 second-factor authentication flow”

Registration flow

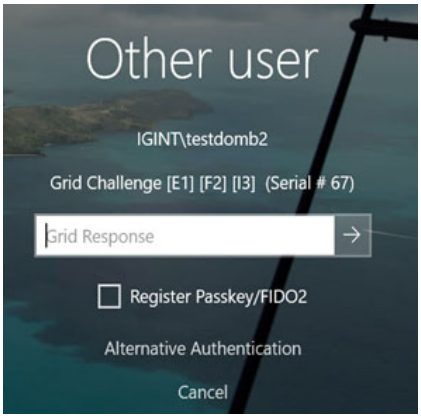
A user can register a Passkey/FIDO2 token once with the same YubiKey using any second-factor authenticator.

If user attempts to register multiple Passkey/FIDO2 tokens, a *Security key already registered* error appears.

The following example shows the Passkey/FIDO2 registration flow.

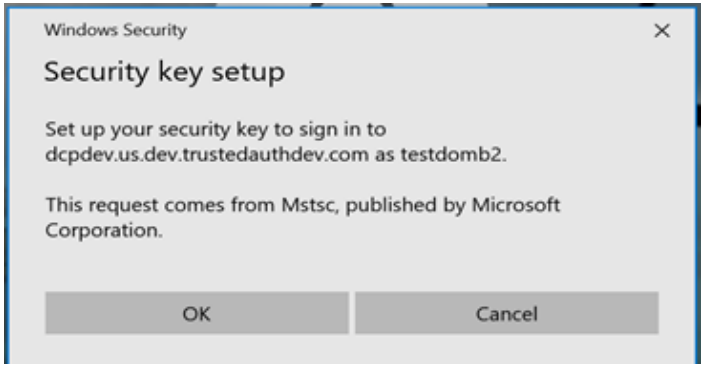
1. User tries to log in and is presented with the password field and sign-in option.
2. User logs in with their username and password.

3 They respond to the second-factor challenge and select **Register Passkey/FIDO2**.

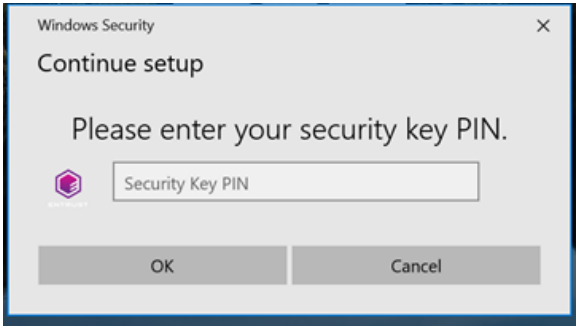


4 If authentication is successful, the user can register their Passkey/FIDO2 token.

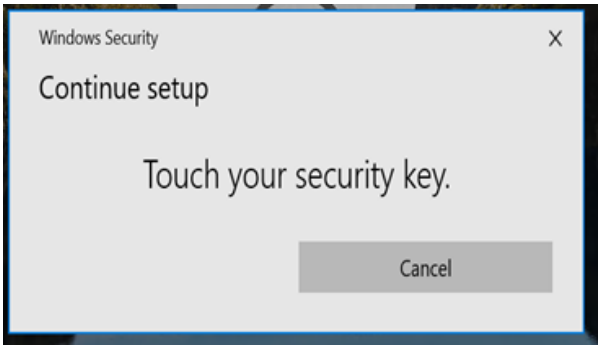
5 The user clicks **OK** on the **Security key setup** prompt.



6 The user enters the **Security Key PIN** and then clicks **OK**.

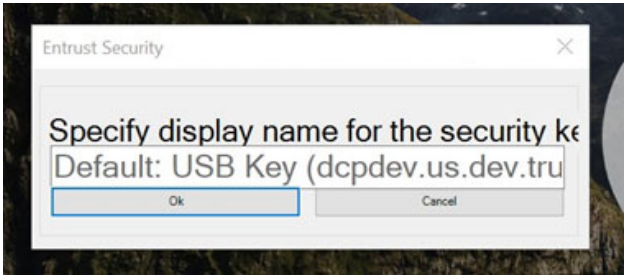


7 The user is prompted to **Touch the security key**.



8 The user taps the security key and is then prompted to enter the display name for the security key.

9 The user enters the display name and then clicks **OK**.



10 The user sees a **Security key is registered successfully** prompt and is logged into Entrust Desktop for Windows.

11 After successful registration, the user logs into Identity as a Service.

12 When the user clicks the **Authenticators** tab on their profile page, they should see the registered Passkey/FIDO2 token.

Passkey/FIDO2 second-factor authentication flow

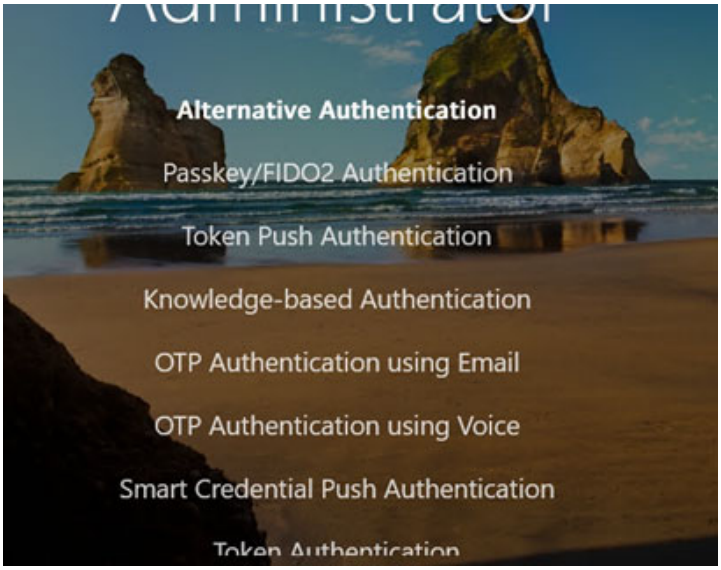
If available, users can authenticate by using their Passkey/FIDO2 token from the second-factor page to log in to Entrust Desktop for Windows, as follows:

1 The users plugs the Yubikey into their laptop.

2 The user tries to log in and is presented with the password field and sign-in options.

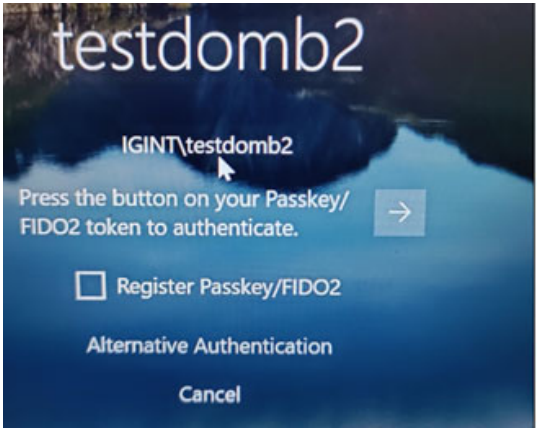
3 The user logs in with their username and password.

4 The user selects **Passkey/FIDO2 Authentication** from the list of second-factor authenticators.The **Passkey/FIDO2 authentication** screen

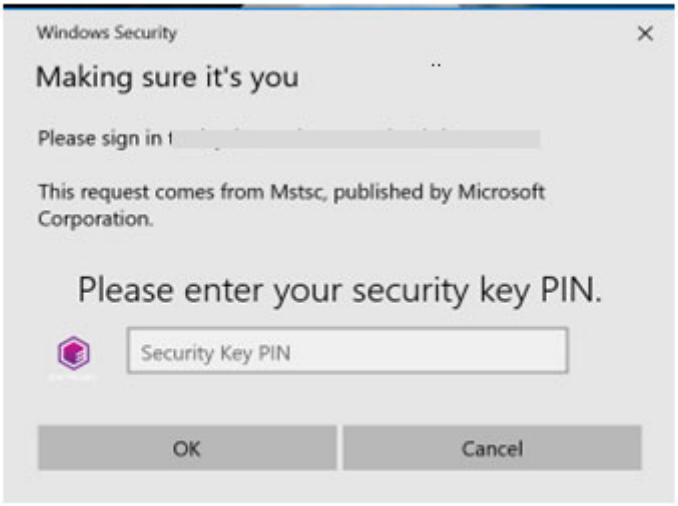


appears.

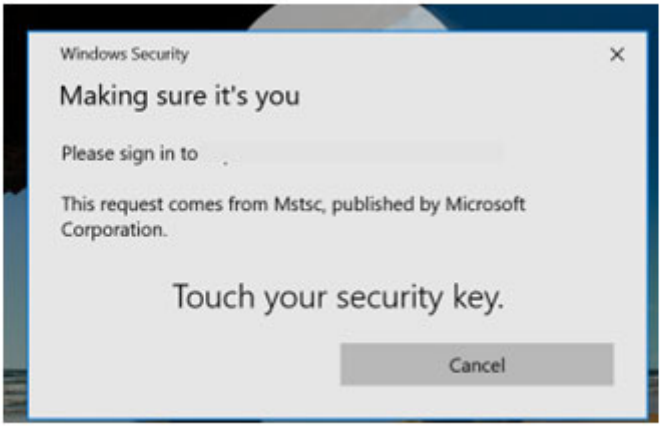
5 The user presses the button on their Passkey/FIDO2 token to authenticate.



6 The user is prompted to enter their **Security Key PIN** and then clicks **OK**.



7 The user touches the security key to confirm their identity.



8 The user is successfully logged in to Entrust Desktop for Windows.

Reset a Passkey/FIDO2 Yubikey

To reset a Yubikey PIN, users can install the Yubikey manager software to change or rest their PIN.

Passkey/FIDO2 authentication with Entrust Identity Enterprise

Windows login supports Passkey/FIDO2 authentication as a second-factor authenticator using physical USB keys (YubiKey) with Entrust Identity Enterprise.

Passkey/FIDO2 registration with Entrust Identity Enterprise can only be done from the Entrust Identity Enterprise Self-Service Module and not from Desktop for Windows.

Passkey/FIDO2 is supported for second-factor authentication for the following:

- Remote Desktop (RDP) and Remote Desktop CREDUI
- Windows console login and Console CREDUI login

Attention:
For instructions on how to configure a Passkey/FIDO2 authenticator, see the *Entrust Identity Enterprise Server 13.0 Server Administration Guide* available on Entrust TrustedCare.

Configure FIDO2/Passkey authentication

Complete the following to configure Passkey/FIDO2authentication:

- “Configure Passkey/FIDO2 in the Entrust Identity Enterprise Self-Service Module” on page 127
- “Configure Passkey/FIDO2 policies in Wed Admin” on page 128
- “How does Passkey/FIDO2 authentication flow work with Entrust Identity Enterprise?” on page 130

Configure Passkey/FIDO2 in the Entrust Identity Enterprise Self-Service Module

Note:
For additional help, see the *Entrust Identity Self-Service Module Installation and Configuration Guide* available at Entrust TrustedCare.

1. Log in to the Entrust Identity Enterprise Self-Service Configuration interface.
2. From the menu at the top, click **Properties**.
3. From the **Table of Contents**, click **FIDO2 Passkey Configuration**.
4. In the **FIDO2 Passkey Configuration** section, complete the following fields:

a Set **Self-Service Module Passkey Authentication Enabled** to **True**.

b Set the **Passkey Authentication Security Level** to **Normal**.

c Set **Passkey Provides Second-Factor Authentication** to **True**.

d Set **Passkey Allow Origin Subdomain** to either **True** or **False**.

e Set **Passkey Allow Origin Port** to **True**.

Note:
The user must create a FIDO Token with a Passkey Relying Party ID that is the same as the value of the Entrust Identity Enterprise Self-Service Module properties and the value passed in PasskeyRelyingPartyID registry of Entrust Desktop for Windows.

5 Click **validate & Save**.

6 From the menu at the top, click **Administration**. The **Administration** page appears.

7 From the **Table of Contents**, select **Passkey Self-Administration**.

8 In the **Passkey Self-Administration** section, select **Yes** for the following question:

Do you want to allow users to register for passkey authentication? If yes, the property "Passkey Relying Party ID" in the "FIDO2 Passkey Configuration" properties group found in the Properties tab must be set correctly.

9 Restart the SSM service for the changes to take effect.

Configure Passkey/FIDO2 policies in Wed Admin

Note:
For additional help, see the *Entrust Identity Enterprise Administrator Guide* available at Entrust TrustedCare.

1 Log in to the Entrust Identity Administration Enterprise Administration Interface as an administrator.

2 Click the **Policies** tab. The **Policies List** page appears.

3 Click the name of the policy that you want to change. The **View Policy** page appears.

4 On the **View Policy** page, click **Edit Policy**. The **Edit policy** information page appears.

5 Set the **Policy Category** settings, as required.

a Select how the passkey should perform User Verification when authenticating with or registering a passkey. The options include:

– Preferred. The relying party prefers user verification but does not fail the response if it does not occur.

– Discouraged. The relying party does not use user verification and avoids it, if possible.

– Required. The relying party requires the user to perform verification.

b Select Discoverable Resident Key (user identity stored) to set whether the Passkey stores a user's identity to allow the user to avoid having to enter their user ID. The options include:

– **Preferred.** The user's identity is stored, if possible.

– **Discouraged.** The user's identity is not stored, if possible.

– **Required.** The user's identity must be stored on the passkey and the user can avoid having to enter their user ID.

c Select the **Authenticator Attachment** to set whether the passkey is embedded on the device or stored externally. The options include:

– **Either.** The passkey can be embedded on either the device or stored externally.

– **Platform.** The passkey is embedded on the device, for example, a Windows laptop.

– **Cross-Platform.** The passkey is stored externally, for example, on a Yubikey or a smartphone.

Note:
Authenticator Attachment applies only to passkey registration and not passkey authentication.

d Enter the **Maximum number of passkeys per User**. The default is 3.

e Enter the **Passkey Challenge Lifetime** to set the time (in seconds) a user has to respond to the challenge before it expires. The default is 180 seconds (3 minutes).

f Select **Disable Challenge Retention** to present the user with a new passkey challenge each time a challenge request is made by the user regardless of whether a currently existing challenge has timed out.

The default is set to **false**. When disabled, the user is presented with the same passkey challenge that previously timed out. Entrust recommends the default setting.

g Select **Update Lockout for Replaced Challenge** to increment the lockout count if an existing challenge is replaced by a new one, either because the current challenge has expired or Disable Challenge Retention is `true`. The default value is `false`.

6 Click **Save Changes**.

7 Click **OK** on the confirmation prompt.

8 Click **Done**.

How does Passkey/FIDO2 authentication flow work with Entrust Identity Enterprise?

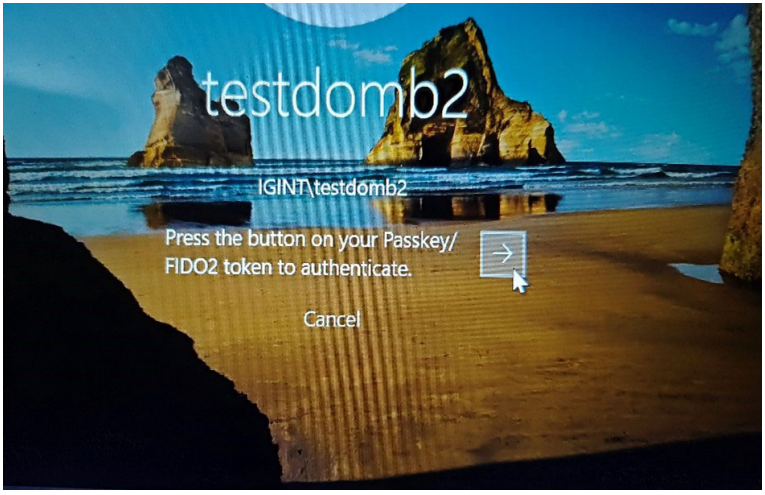
User can authenticate by using a Passkey/FIDO2 as a second-factor authenticator to log in to Entrust Desktop for Windows.

How it works

1 The users plugs the Yubikey into their laptop.

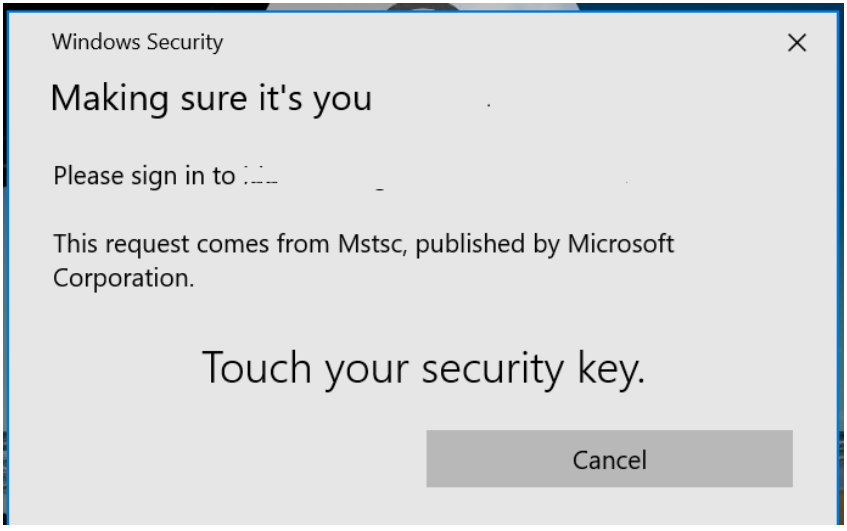
2 The user logs in with their username and password.

3 The user is presented with the Passkey/FIDO2 authentication screen.



4 The user is prompted to enter their **Security Key PIN** and then clicks **OK**.

5 The user touches the security key to confirm their identity.



6 The user is successfully logged in to Entrust Desktop for Windows.

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 a use a

personal verification number (PVN) with the token for additional security. See “Personal verification numbers” on page 167.

Authentication works a little differently for the two token types.

Response-only tokens

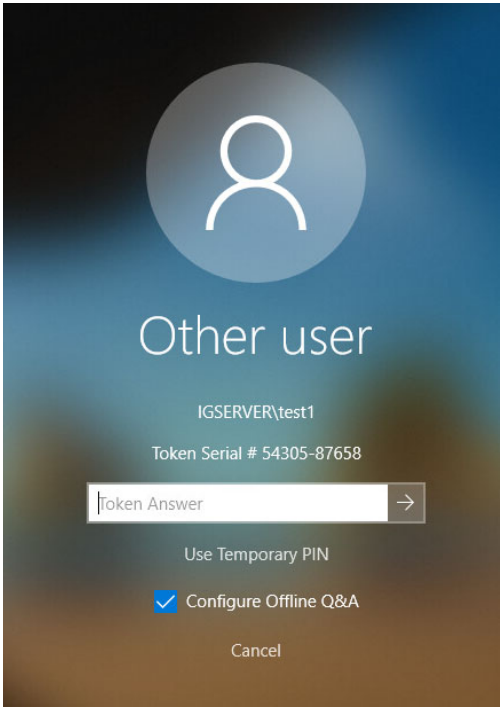
For response-only tokens, authentication works as follows:

1. The user completes first-factor authentication successfully.
2. Entrust 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 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 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 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 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 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 210 for more information.

OTP manual authentication works as follows:

1. The user completes first-factor authentication successfully.
2. Entrust presents the user with a challenge based on their OTP.
3. The user contacts the Entrust 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 or Identity as a Service.

Mobile soft token (TVS) authentication

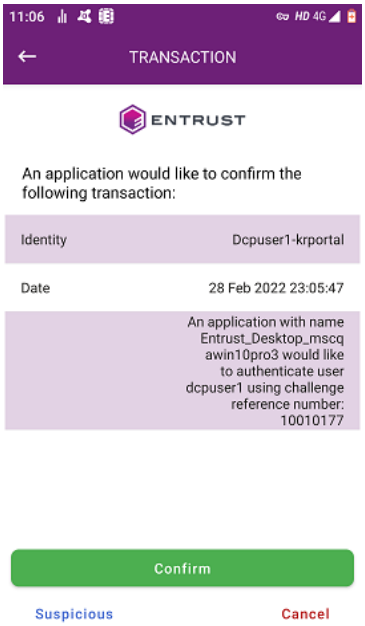
The Entrust Identity Enterprise Mobile Soft Token app generates numbers that you use to authenticate to a Web site or to confirm transactions.

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 Identity Enterprise or Identity as a Service 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.

Customizing push authentication text messages

You can customize the text that appears on the soft token application for push authentication.

To modify the text for push authentication messages

1 Follow the steps in the section,"Customizing Entrust Desktop error messages and second factor user-visible text" on page 187 to modify the text for the resource ID, `IDS_RO_MOBILEST_MESSAGE_PREFIX`.

Notification text can additionally contain embedded format specifiers that are replaced by the values specified in the output. See the following examples:

a Example 1:

Format Specifier: `{HOST_NAME}`

Output: Replaced with host name in the specified location or locations.

Example:

ResourceID Text: `An application with name Entrust_Desktop_{HOST_NAME} would like to authenticate user.`

Push Notification Text: `An application with name Entrust_Desktop_Windows10DevSys would like to authenticate user.`

b Example 2:

Format Specifier: `{USER_NAME}`

Output: Replaced with user name in the specified location or locations.

Example:

ResourceID Text: `An application with name Entrust_Desktop_{HOST_NAME} would like to authenticate user {USER_NAME}.`

Push Notification Text: `An application with name Entrust_Desktop_Windows10DevSys would like to authenticate user TestUser1.`

c Example 3:

Format Specifier: `{CHALLENGE_REFERENCE_NUMBER}`

Output: Replaced with challenge reference number in the specified location or locations.

Example:

ResourceID Text: `An application with name Entrust_Desktop_{HOST_NAME} would like to authenticate user {USER_NAME}  using challenge reference number: {CHALLENGE_REFERENCE_NUMBER}.`

Push Notification Text: `An application with name Entrust_Desktop_Windows10DevSys would like to authenticate user TestUser1  using challenge reference number: 100X0X01.`

d Example 4:

Format Specifier: {FQDN}

Output: Replaced with fully qualified domain name in the specified location or locations if available; otherwise, replaced with host name.

Example:

ResourceID Text: `An application with name {FQDN} would like to authenticate user {USER_NAME}  using challenge reference number: {CHALLENGE_REFERENCE_NUMBER}.`

Push Notification Text: `An application with name Windows10DevSys.example.com would like to authenticate user TestUser1  using challenge reference number: 100X0X01.`

Configure Entrust Desktop for Windows for Soft Token with mutual challenge

Mutual authentication challenge requires users to respond to a mutual push authentication challenge. When enabled, users must match the challenge that appears on the second-factor page of Entrust Desktop for Windows with the mutual challenge shown in their Entrust Identity app.

This procedure assumes that you have already integrated Entrust Desktop for Windows with Identity as a Service. See “Configuring the Entrust Identity Enterprise or Identity as a Service settings” on page 39.

Topics in this section:

Configure soft token for mutual challenge in Identity as a Service

To complete this procedure you need to log in to your IDaaS Administrator account and open the Administration Help.

To configure soft token for mutual challenge

1. Log in to Identity as a Service as an administrator.
2. Go to **Home >Policies > Authenticators > Entrust Soft Token**. The **Entrust Soft Token Authenticator** page appears.
3. Select **Enable Mutual Challenge** for Entrust Soft Token authenticator.

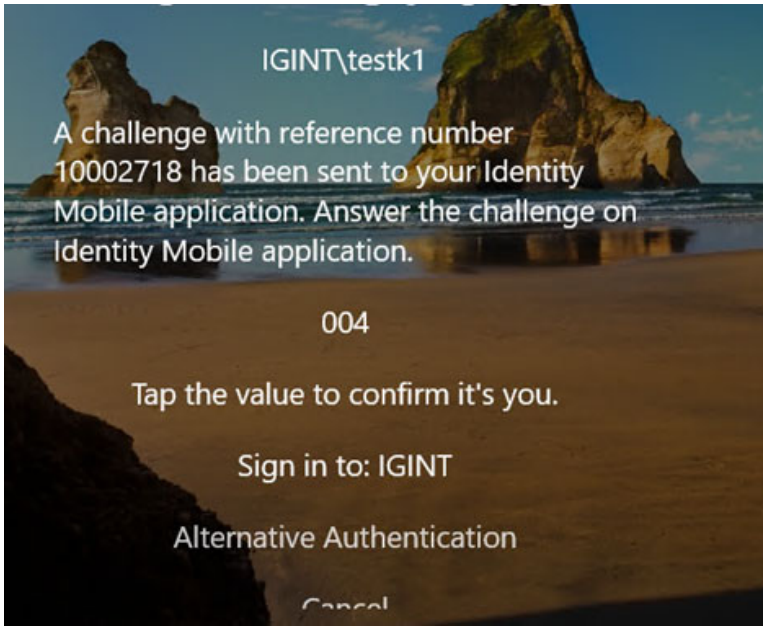
   See Modify Entrust Soft Token authenticator in the *Identity as a Service Administrator Online Help* for more information.
4. Create a custom authentication flow with **External Authentication** set for first-factor and **Entrust soft token push** for second-factor authentication. See Create authentication flows in the *Identity as a Service Administrator Online Help*.
5. Using the authentication flow you created, create a resource rule to protect Entrust Desktop for Windows for mutual challenge authentication with IDaaS.

   See Create resource rules in the *Identity as a Service Administrator Guide*.

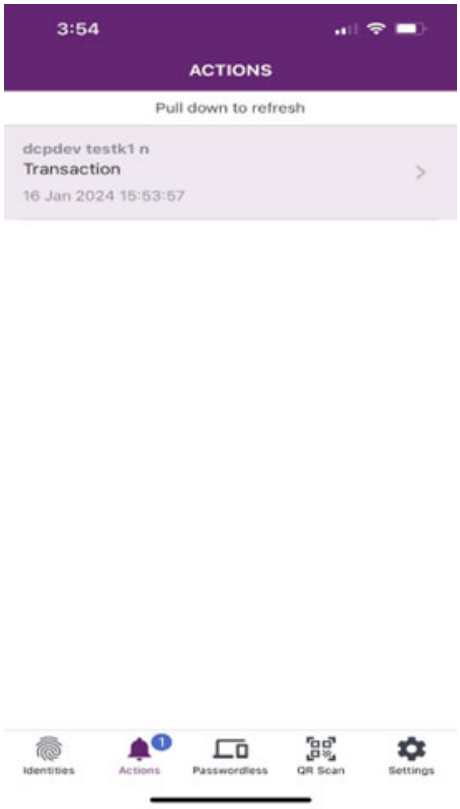
How soft token with mutual challenge works

1. The user accesses Entrust Desktop for Windows and enters their username and password in the first-factor page.

2 On the second-factor page, the mutual authentication push token challenge number appears.

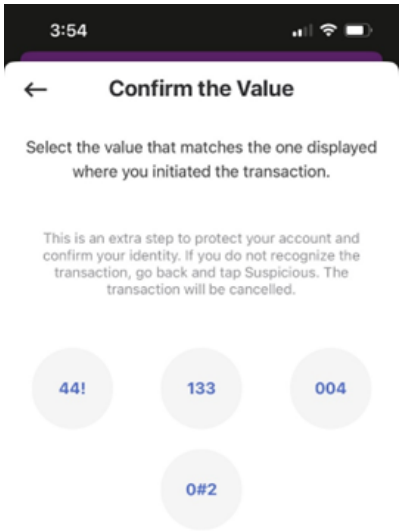


3 The user receives the notification on their mobile device in the Entrust Identity app.



4 The user clicks the **Actions** button to see more about the request and then clicks **Confirm**.

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



6 After successful authentication, the user is automatically logged into Entrust Desktop for Windows.

7 The user must return to the first-factor authentication page if mutual authentication is unsuccessful.

Mobile Smart Credentials authentication

Mobile Smart Credentials authentication is a strong out-of-band authentication method where an authentication challenge is sent to the user's mobile. This challenge is signed by the Entrust Mobile smart card app and verified by Entrust. A user can accept or reject the challenge, which results in either a successful or failed authentication.

Smart Credential authentication works as follows:

1. The user completes first-factor authentication successfully.
2. Entrust Desktop presents the user with a challenge that has been sent to their mobile smart credential application. .
3. Open the Entrust Mobile Smart Credentials app on your mobile device.
4. Optionally a notification is sent to the user's mobile application to indicate that a security challenge is available.
5. If a security challenge is available, the mobile smart credential application fetches the security challenge. If required, the mobile application prompts the user for the smart credential PIN to authenticate that they can access the smart credential. The smart credential is used to authenticate the mobile application to Entrust Identity Enterprise or Identity as a Service to prove that they have access to download the security challenge.
6. The mobile smart credential application displays the security challenge allowing the end user to confirm, concern or cancel the challenge. The user can select Confirm to allow the authentication to proceed, Cancel to abort the authentication, or Concern, to report the authentication as suspicious (possibly because they did not initiate the authentication).
7. Click **Next** button in Entrust Desktop application to access the resource.

Risk-based authentication

The Entrust Desktop solution allows you to use Entrust Identity Enterprise and Identity as a Service risk-based authentication (RBA). You can define the RBA settings you want during installation of the solution. See the *Entrust Identity Enterprise Administration Guide* and the *Identity as a Service Admin Help* for more information about risk-based authentication policies and the "`EnableRBAAuth`" on page 212 registry key for more information on enabling RBA.

Note:
The `EnableRBAAuth` setting supports console only with machine authentication.

For integrations with Identity as a Service, configure Machine Authentication only in the resource rule. For Identity Enterprise integrations, do not configure IP Authentication Tests.

Topics in this section:

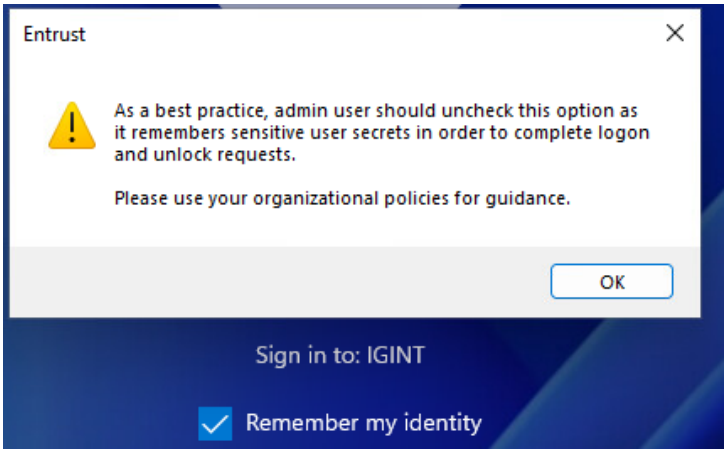
How RBA works

When enabled, users see a **Remember my identity** and **Clear my identity** on the first-factor screen.

When RBA is enabled, **Remember my identity** is always unchecked for first time users. After a user registers machine data in either Entrust Identity Enterprise or Identity as a Service, **Remember my identity** is checked by default.

RBA is disabled in the following circumstances and the **Remember my identity** and **Clear my identity** check boxes do not appear on the first-factor page:

- If `EnableRBAAuth` and `EnableCombinedAuth` are set to `1`
- If `EnableRBAAuth` and `EnablePwdless` are set to `1`
- If `EnableCombinedAuth` and `EnablePwdless` are set to `1`



Note:
Machine secrets are deleted from the registry when a user checks the **Clear my identity** checkbox. This checkbox can be used to clear the machine secrets on Entrust Desktop for Windows. The next time a user checks the **Remember my identity** checkbox, Entrust Desktop for Windows requests to register the machine again.

User experience with Entrust Identity Enterprise

Remember My Identity and **Clear my identity** are available only in the Console mode **LOCK** and **UNLOCK** use cases. It is disabled for remote desktop, credential UI, and passwordless login.

The following describes the user experience with Console Login (Lock and Unlock scenario) with Entrust identity Enterprise.

When using RBA with IDG, Entrust recommends the following:

If a user uses remote desktop login, their trusted IP can only be cleared in Entrust Identity Enterprise. **Clear my identity** clears only the machine secrets from Entrust Desktop for Windows and not the trusted IP from Entrust Identity Enterprise.

To clear the Trusted IP, users do the following:

1 Log in to Entrust Identity Enterprise.

2 Navigate to **User Account > Authentication Types**.

3 Select **Location**.

4 Delete the IP Address from Location History.

Prerequisites for RBA with Entrust Identity Enterprise

1 The following provides an example of the policy setting to use RBA with Entrust Identity Enterprise:

   a Under **Policies >Machine Secret** set the following:

   – Maximum Number of Machine Secrets = 1

   – Sequence Nonce Required = Yes

   – Machine Nonce Require = Yes

2 Under **Risk-Based Authentication**, select one of the following:

- If IP Authentication does not fail and Certificate Authentication does not fail and Machine Authentication passes and External Risk Authentication does not fail
- IP Authentication does not fail and Certificate Authentication passes and Machine Authentication does not fail and External Risk Authentication does not fail
- IP Authentication passes and Machine Authentication passes

First time login user experience

1 The user enters their username and password.

2 The user selects the **Remember my identity** checkbox and then clicks **Submit**.

3 First-factor authentication validates successfully.

4 The user is prompted for second- factor authentication from first and **Available Authentication Types IDE Policies**.

5 The user enters the correct second-factor authenticator.

6 Entrust Desktop for Windows validates with Entrust Identity Enterprise.

7 Entrust Identity Enterprise authentication is successful and responds with the machine secrets.

8 Machine secrets are saved in the registry for the user and the user is allowed to log in.

Second consecutive login user experience

In this example, **Remember my identity** is checked by default because the machine secrets are saved in the registry.

1. The user enters their username and password.
2. **Remember my identity** is selected by default.
3. The user clicks **Submit**.
4. First-factor authentication validates successfully.
5. The user is not prompted for second-factor authenticator.
6. Entrust Desktop for Windows validates the machine secrets saved in the registry with Entrust identity Enterprise.
7. Entrust Identity Enterprise authentication is successful and responds with machine secrets.
8. Machine secrets are saved in the registry for the user and the user is allowed to log in.

User experience if the User Machine Secret has expired in Entrust Identity Enterprise

1. The user enters their username and password.
2. **Remember my identity** is selected by default.
3. The user clicks **Submit**.
4. First-factor authentication validates successfully.
5. User is prompted for second- factor authentication from first and **Available Authentication Types IDE Policies**.
6. The user enters the correct second-factor authenticator.
7. Entrust Desktop for Windows validates with Entrust Identity Enterprise.
8. Entrust Identity Enterprise authentication is successful and responds with the machine secrets.
9. Machine secrets are saved in the registry for the user and the user is allowed to log in.
10. On the next consecutive logins, the user is not prompted for second-factor if Entrust Desktop for Windows validates the machine secrets saved in the registry with Entrust Identity Enterprise and Entrust Identity Enterprise authentication is successful and responds with the machine secrets.
11. Machine secrets are saved in the registry for the user and the user is allowed to log in.

User experience with Identity as a Service

The following describes the user experience with IDaaS for Console Login with machine secrets and IP authentication (LOGIN and UNLOCK scenarios).

Recommendations when using RBA with IDaaS

When using RBA with IDaaS, Entrust recommends the following:

1. If a user uses remote desktop login, their trusted IP can only be cleared in IDaaS.
2. Clear my identity clears only the machine secrets from Entrust Desktop for Windows and not the trusted IP from IDaaS.
3. To clear the Trusted IP, users must do the following:
   a. Log in to their IDaaS account.
   b. Go to their **My Profile** page.
   c. Select the **Risk-Based Authentication** tab.
   d. Delete the IP Address.
4. If using RBA with Knowledge-based authentication, set KBA to high risk in the IDaaS resource rule.
5. Enable the setting for **Do not use IP Address for Resource Rule Risk Factors** for the IDaaS Desktop Application for RBA and Non-RBA user login.

Prerequisites for IDaaS

The following provides an example of recommended resource rule settings that should be configured before enabling RBA. In order to test RBA with Entrust Desktop for Windows, use only the following two risk factors:

- Machine Authenticator
- Location History

Set these risk factors so that the sum of them always equals 100%. For example, set Machine Authenticator to 70% and Location History to 30%.

Note:
Device Fingerprint available under Machine authenticator is not supported for RBA authentication in both Entrust Identity Enterprise and Identity as a Service.

The following settings are mandatory for RBA authentication with IDaaS:

1. Log in to your IDaaS admin account.

2 Click **Home > Policies > Authenticators > Machine Authenticator**. The **Machine Authenticator** page appears.

3 Set the **Machine Authenticator Required for Machine Registration** to **Password**.

4 Click **Save**.

First time login experience (Remember my identity **is unchecked by default)**

1 The user enters their username and password.

2 The User selects the **Remember my identity** checkbox and then clicks **Submit**.

3 First-factor authentication validates successfully.

4 The user is prompted for second- factor authentication from the high risk authenticators configured in the resource rule.

5 The user enters the correct second-factor authenticator.

6 Entrust Desktop for Windows validates with IDaaS.

7 Entrust Desktop for Windows sends the IP address of the machine.

8 IDaaS authentication is successful and IDaaS responds with machine secrets and then adds the Entrust Desktop for Windows IP to the list of trusted IPs.

9 Machine secrets are saved in the registry for the user and user is allowed to log in.

Second time login

In this example, **Remember my identity** is checked by default because the machine secrets are saved in the registry.

1 The user enters their username and password.

2 **Remember my identity** is selected by default.

3 The user clicks **Submit**.

4 First-factor authentication validates successfully.

5 Second-factor authentication occurs as follows based on the resource rule:

If the resource rule has been configured for low risk:

a IDaaS prompts the user for second-factor authentication from the list of low risk authenticators.

b The user enters the correct second-factor authentication response.

c IDaaS validates the second-factor authentication successfully.

d Entrust Desktop for Windows sends the IP address of the machine to IDaaS.

If the resource rule has not been configured for low risk:

a IDaaS does not prompt the user for second-factor authentication.

b User is not prompted for second-factor authentication.

c Entrust Desktop for Windows validates the machine secrets saved in the registry with IDaaS.

d Entrust Desktop for Windows sends the IP address of the machine to IDaaS.

e IDaaS validates the IP address successfully.

f IDaaS authentication is successful and responds with the machine secrets.

g Machine secrets are saved in the registry for the user and user is allowed to login.

User experience if the User Machine Secret has expired in IDaaS

1. The user enters their username and password.
2. Remember my identity is selected by default.
3. The user clicks **Submit**.
4. First-factor authentication validates successfully.
5. User is prompted for second-factor authentication from the first available authenticator under High Risk in the resource rule.
6. The user enters the correct second-factor authenticator.
7. Entrust Desktop for Windows validates with Identity as a Service.
8. Identity as a Service authentication is successful and responds with the machine secrets.
9. Machine secrets are saved in the registry for the user and the user is allowed to log in.
10. If the resource rule has not been configured for low risk, on the next consecutive logins, the user is not prompted for second-factor if Entrust Desktop for Windows validates the machine secrets saved in the registry with Identity as a Service and Entrust Identity as a Service authentication is successful and responds with the machine secrets.
11. If the resource rule has been configured for low risk, on the next consecutive log in attempts the user is prompted for a second-factor authenticator configured under low risk in the resource rule.
12. Entrust Desktop for Windows validates the machine secrets saved in the registry with Identity as a Service and Identity as a Service authentication is successful and responds with the machine secrets.
13. Machine secrets are saved in the registry for the user and the user is allowed to log in.

Authenticate CREDUI registry to authenticate elevated login (RDP)

When Entrust Desktop for Windows is installed on the server and RBA is enabled, the end user should be prompted for MFA once for all elevated (CREDUI) login scenarios.

For example, a user tries to RDP from one machine to another using a mstsc tool. For first time login the user is prompted for MFA once. From the second time onwards, the user bypasses second-factor authentication.

CredUI works as expected if the IP captured for the user under IDaaS is the IP address of the source machine for console login and the RDP client IP address for RDP login.

When there are multiple IP adresses for the RDP client machine, the IP address reported by the RDP client is trusted for RBA authentication.

How it works

The user needs to be the same as the console/Windows login. See the Entrust Identity Administration Guide to configure RBA for Entrust Identity or the Entrust Identity as a Service Administrator Help to configure RBA for IDaaS. See also "How RBA works" on page 144.

The following is an example of CREDUI with RBA.

Prerequisites

- Install Entrust Desktop for Windows on machine A and machine B.
- On both machines A and B, enable `EnableRBAAuth` and `AuthenticateCredUILogin` to `1`.
- In the **IntelliTrust Desktop** application on IDaaS, set the **Source of Client IP Address for Risk Conditions** to **Provided in the API**.
- Enable the checkbox **Check the IP Address in location history** in the IDaaS policy settings.
- In the IDaaS resource rule, do the following:
  - Set the **Location History** to 100% in resource rule.
  - Enable RBA and set the second-factor for high risk and medium risk.
  - Set low risk to **None**.
  - Steps:

Console Login

1 Log in to Machine A with a valid username and password and check the Remember my Identity checkbox.

2 The user responds to second-factor authentication to login. The IP is remembered for the user in IDaaS.

Elevated / RDP Login

After successfully completing user log in with multi-factor authentication, a user tries to log in to any elevated login or a remote machine and gets a login pop-up.

The following occurs when the same user does elevated login:

1 The user provides their username and password, and then clicks on the Remember my Identity checkbox.

2 The user is not prompted for second-factor authentication as the source IP is already trusted.

Registry entries

The RBA data is located in:

`HKEY_LOCAL_MACHINE\Software\Entrust\WIGL\Users\userSID\RBA`

The registry entry for **Remember My Identity** is located in:

`HKEY_LOCAL_MACHINE\Software\Entrust\WIGL\UserSettings`

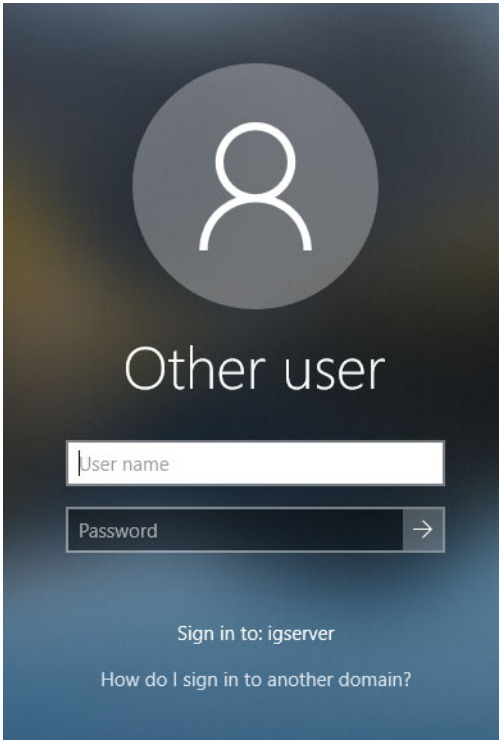
Passwordless authentication

1 The log in screen displays the user's user name.

Entrust Desktop for Windows users begin logging into the domain by entering their user name and their Windows password. Entrust Identity Enterprise Windows users must have a valid Windows userid in the protected domain. Users logging into the domain must be registered as a user in Entrust protecting the domain. Unregistered users may be treated differently (see "Users without Entrust" on page 174).

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. The following example shows a grid challenge in Entrust Identity Enterprise.

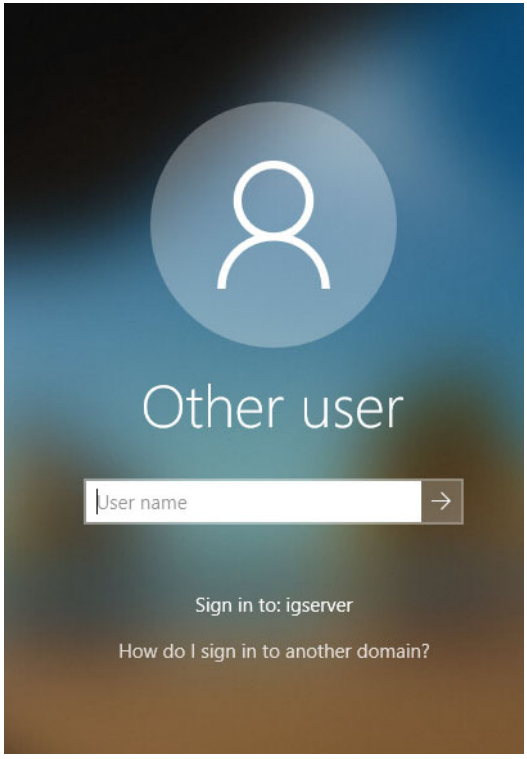


Note:
After the user clicks the arrow button and the second-factor authentication screen appears, they cannot return to the first-factor login screen. If the user decides to back-out of second-factor authentication without completing the challenge, they must use the **Switch User** button.

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 Identity Enterprise or Identity as a Service.



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

Note:
Passwordless login is supported in the CREDUI only with Entrust Identity Enterprise.

Online Question and Answer (Q&A)

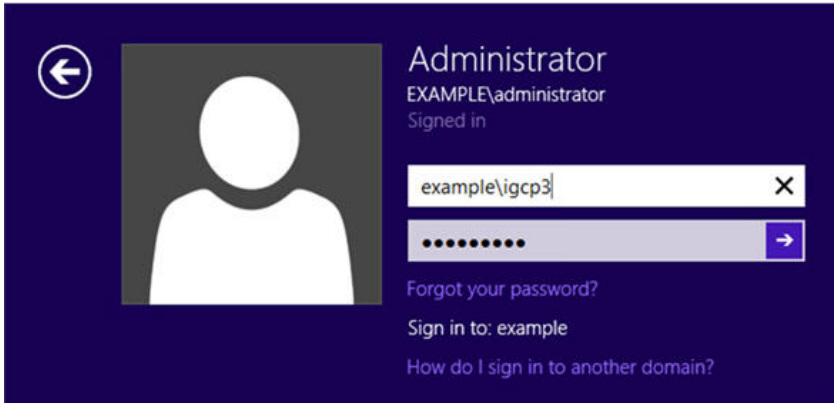
Before Q&A can be configured for use on the user's computer, the user's profile on the Entrust Identity Enterprise or Identity as a Service must have Q&A set up and the minimum number of challenges must be configured. This can be done using Entrust Identity Enterprise Self-Service Module or directly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

See the Entrust Identity Enterprise *Administration Guide* or the *Identity as a Service Administrator Online Help* for more information.

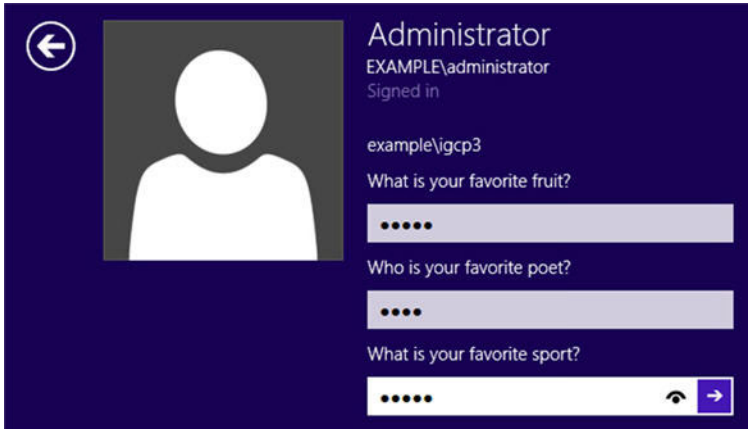
Like any authentication method, Q&A must be set up online (allowing the challenge to be saved locally) before it can be used offline.

To set up Q&A

1 The user logs in and successfully completes 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 Identity Enterprise or Identity as a Service 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 Identity Enterprise or Identity as a Service must have Q&A set up and the minimum number of challenges must be configured. This can be done using Entrust Identity Enterprise Self-Service Module or directly on the Entrust Identity Enterprise or Identity as a Service. See the *Entrust Identity Enterprise Administration Guide* or *Identity as a Service Administration Online Help* for more information.

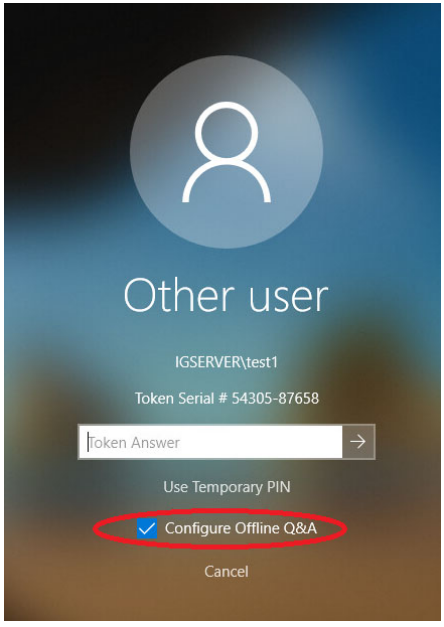
To configure Q&A for offline use as a user option in your Desktop for Windows package, select it when you configure the Entrust Desktop for Windows installation package. See "Using the custom installation wizard" on page 50.

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.

When a user authenticates using Q&A on the second-factor page, only offline Q&A is stored in the registry for the user, and the offline token is not downloaded in this case.

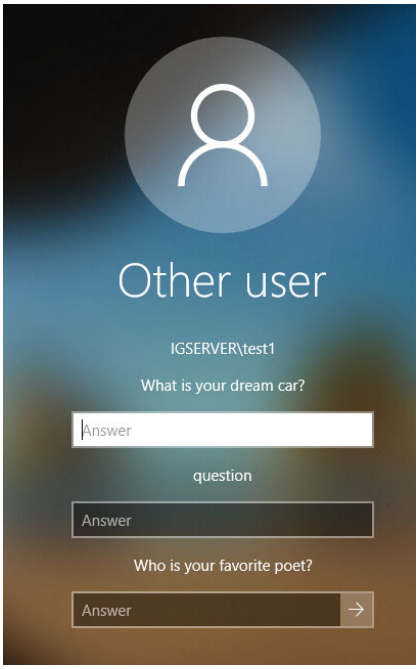
To set up Q&A for offline use

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 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, no Q&A pairs are stored locally. Any previous Q&A pairs are kept.

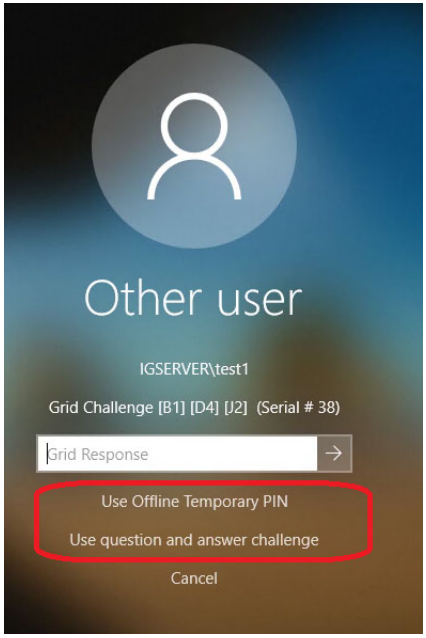
Failing the challenge uses up one of the users authentication attempts. Too many failed attempts could cause the user to be locked out.

If the user updates their Q&A in Entrust, 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.

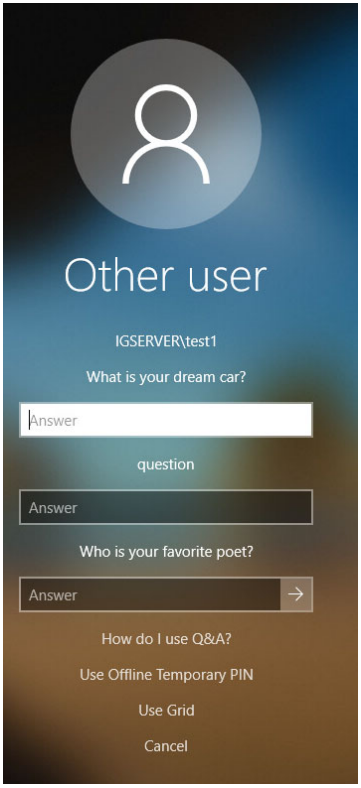
To log in offline using Q&A

1 The user completes first-factor authentication successfully.

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



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



Note:
All answers must be exact. For example, if the answer includes the word `doctor` you must use word `doctor`, not `Dr`. Unlike Entrust Identity Enterprise or Identity as a Service, Entrust Desktop for Microsoft Windows does not support word substitution.

Offline token

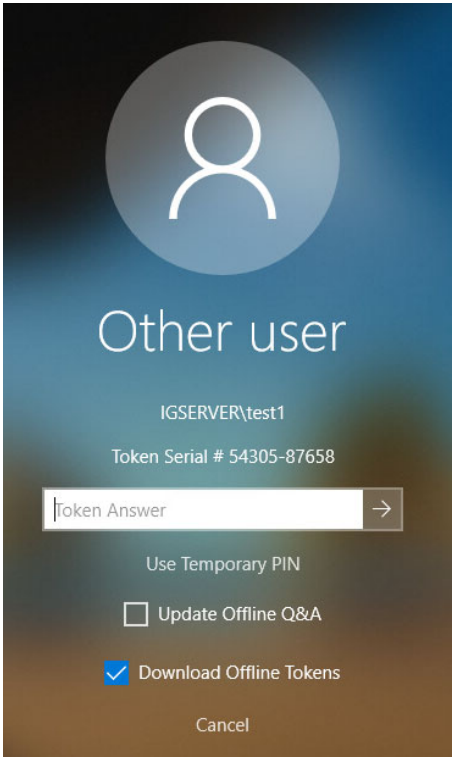
Before token authentication can be configured for offline use on the user's computer, the user's profile on the Entrust must have offline token set up. This can be done using in Identity as a Service or on Entrust Identity Enterprise Self-Service Module directly on the Entrust Identity Enterprise. To 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

Desktop for Windows installation package. See “Using the custom installation wizard” on page 50.

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.



Note:
The Offline OTP hours downloaded for the first time are the hours configured under **Protected Offline OTP Max.** in Entrust Identity Enterprise or **Maximum Offline Time (Hours)** in Identity as a Service.

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 Identity Enterprise or Identity as a Service.

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 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.

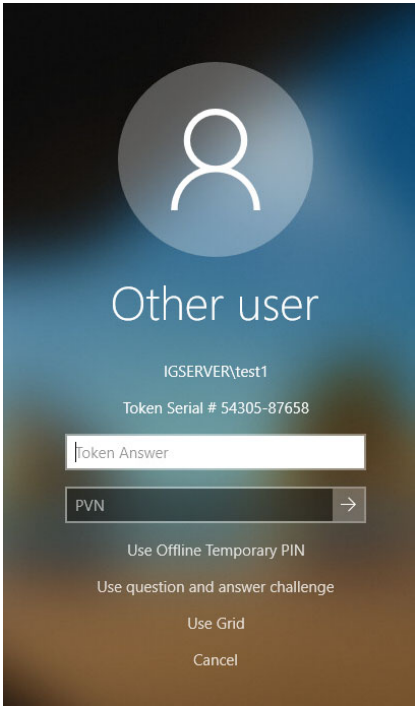
Note:
Failing the challenge uses up one of the users authentication attempts. Too many failed attempts can cause the user to be locked out.

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.



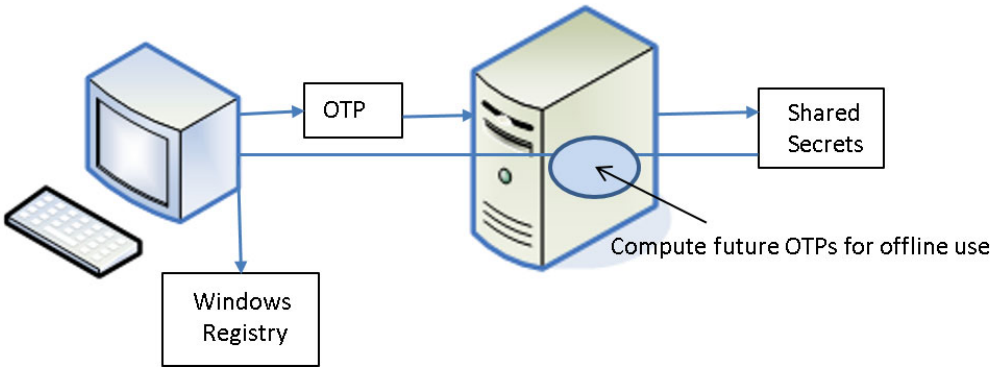
3 The user clicks **Submit**.

How the offline token works

When a user authenticates to Entrust 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 Identity Enterprise or Identity as a Service Authentication, 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 Identity Enterprise or Identity as a Service 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 Identity Enterprise or Identity as a Service).

If the download offline token is checked, it downloads OTPs for Max Hours (according to policy setting in Entrust Identity Enterprise or Identity as a Service).

Display of Offline token validity

The offline token validity (the serial number of the token and the time remaining before the offline token downloaded expires) displays on the first-factor screen if the user has downloaded offline tokens. The offline token validity appears on both the first-factor screen and the second-factor screen if Token Push or soft token authentication is configured for second-factor authentication as the first second-factor authenticator presented to the user.

The following table provides an example of the offline token validity information.

Table 4: Offline token validity messages

Message	Description
Serial #XXXX-1112 : 0 hours remaining	This message is applicable for active tokens before the token is downloaded.
Serial #XXXX-1112 : Expired	This message is available once the downloaded tokens have expired.
Serial #XXXX-1112 : XX.XX hours remaining	Offline token validity

The following screenshots provide examples of what a user will see on the login screens.

Figure 6: Display of offline token validity on the first-factor page

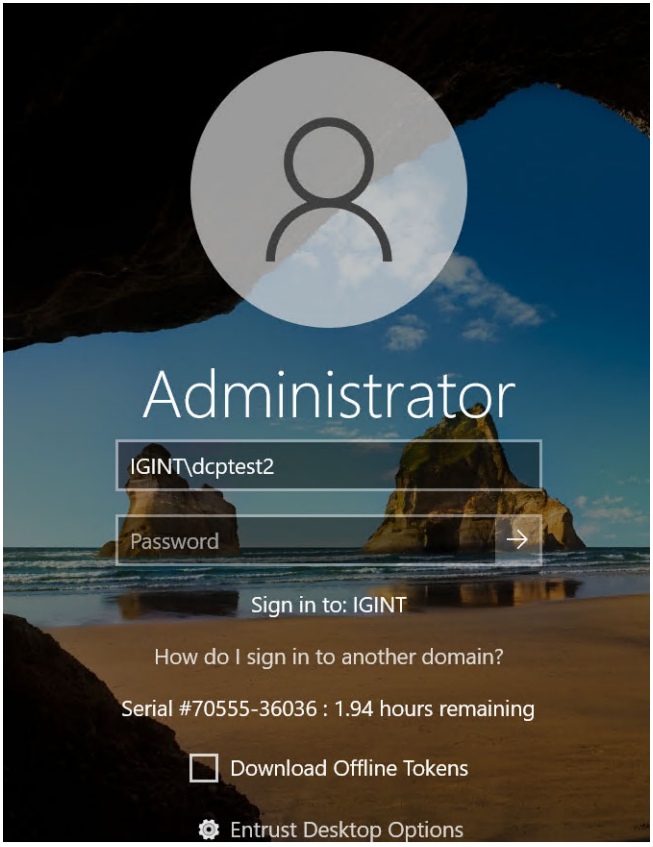
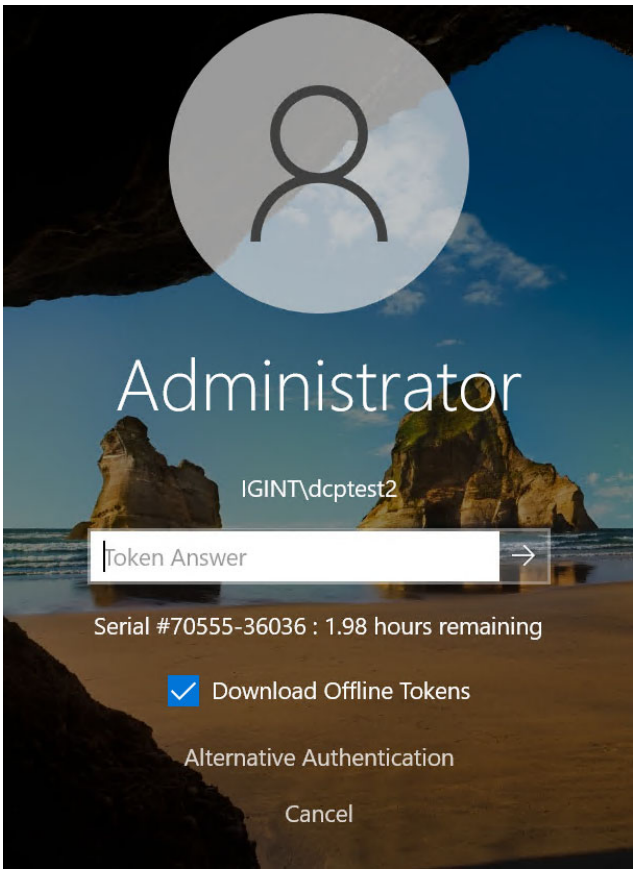


Figure 7: Display of offline token validity on the second-factor page



How offline token works when RBA is enabled

Download Offline Tokens is available under **Entrust Desktop Options** in the first-factor login screen. This feature allows the user to select and download offline tokens while in RBA low risk when Token and Token Push is set in high risk.

Prerequisites for offline token with RBA enabled

- **Download Offline Token** appears under **Entrust Desktop Options** in the first-factor screen to allow the user to download offline tokens.
- **Download Offline Token** appears only if all of the following conditions are met:

  – RBA is enabled.

  - The user has either Token or Token Push second-factor authenticator available under high risk.
  - The user has navigated through high-risk flow at least once.
- This option does not appear for CredUI Login.
- If the user selects this option on the first-factor screen from the **Entrust Desktop Options** Entrust Desktop for Windows displays either Token or Token Push even if user has other second-factor authenticators prior to Token or Token Push authentication.
- By default, this option is unchecked on the first-factor screen.
- This option does not appear in offline mode.
- The **Download Offline Token** checkbox appears in the first-factor screen only when `EnableRBAAuth` and `OfflineOTPDownloadHours` are enabled.
- The **Download Offline Token** checkbox appears for both RDP and console sessions.

How offline token with RBA works

Download Offline Token is not available under **Entrust Desktop Options** when a user logs on to Entrust Desktop Credential Provider for the first time with RBA enabled.

After the user performs a high-risk authentication (the user must have a Token or Token Push authenticator), the following occurs:

- The user's next log on falls under low risk.
- The user can navigate to high-risk flow from the first-factor login screen by deselecting **Remember my identity** and selecting **Download Offline Token**.
- The user is shown either a Software/Hardware Token or the Entrust Soft Token Push authenticator in the second-factor screen.
  - If Software/Hardware Token is set first followed by Entrust Soft Token push, the user is shown whichever token is set first in the resource rule.
- If the user deselects **Download Offline Token** on the first-factor screen and Entrust soft token push appears on the second-factor screen, offline tokens are downloaded.
- If the user checks **Download Offline Token** on the first-factor screen and Software/Hardware Token appears on the second-factor screen, offline

tokens are not downloaded if the user deselects **Download Offline Token** on the second-factor screen.

- If the user deselects **Download Offline Token** on the second-factor under Software/hardware token, the offline tokens are not downloaded.
- If the user deselects **Download Offline Token** on the first-factor screen and Software/hardware token appears on the second-factor screen, offline tokens are downloaded when the user checks **Download Offline Token** on the second-factor screen.
- Once the user has downloaded the offline token through risk-based authentication, subsequent logins display the remaining validity of the offline token.

  If the remaining validity is equal to or less than the threshold value defined in the `OfflineTokenThreshold` registry, then the user is directed to a high-risk authentication flow where token or a token push is presented as the first challenge in the second-factor authentication screen. This occurs if the user has configured either token or token push as a first second-factor authenticator under high risk flow

  After being redirected to high risk, the user should enable **Download Offline Token** in the second-factor screen in order to update the offline token remaining validity to allow the user to continue logging in with the downloaded token whenever the system goes offline.
- Once the token lifetime has expired, the existing RBA flow will follow (it will go to the low risk if the machine secrets have not expired.)

Note:
The `OfflineTokenThreshold` registry setting applies exclusively to Token and Token Push authentication methods. It is not applicable to other types of authenticators.

Personal verification numbers

The personal verification number (PVN) feature provided with Entrust Identity Enterprise 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 Identity Enterprise policy to require PVNs. An administrator can create PVNs for your users, or you can let users create and update their own PVNs.

The PVN can be any length from 1-255 digits, but you should select a length that makes the value easy to remember and enter, while still providing an acceptable

level of security. You set the length in the PVN policy on the Entrust Identity Enterprise.

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.

Temporary PIN authentication

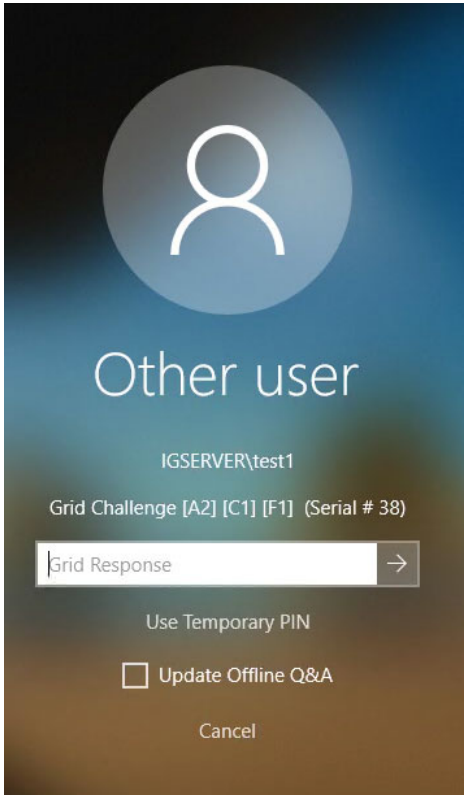
In certain situations, where the user does not have a grid or token, you can issue a temporary PIN, either for a specific number of uses or a limited period of time. Examples of this situation include lost grids or tokens, or a newly registered user waiting for their grid or token to arrive.

Temporary PINs are configured on the Entrust Identity Enterprise. 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.

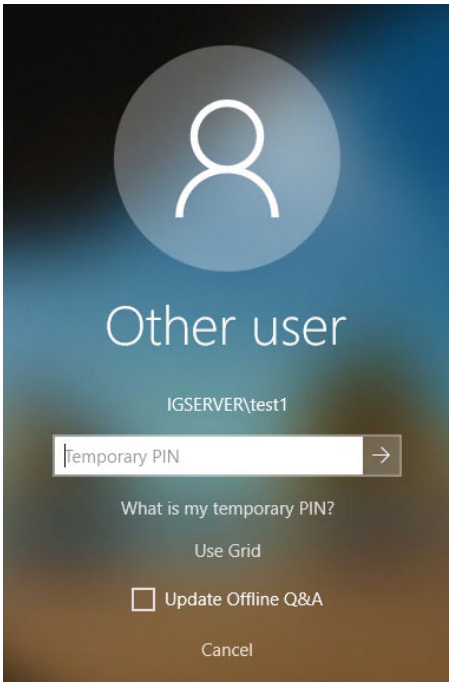
Temporary Access Codes are configured in Identity as a Service. See "Temporary access code" on page 172.

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 201.

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



If the user clicks **Use temporary PIN**, Entrust 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 Identity Enterprise. See the *Entrust Identity Enterprise Administration Guide* for further information.

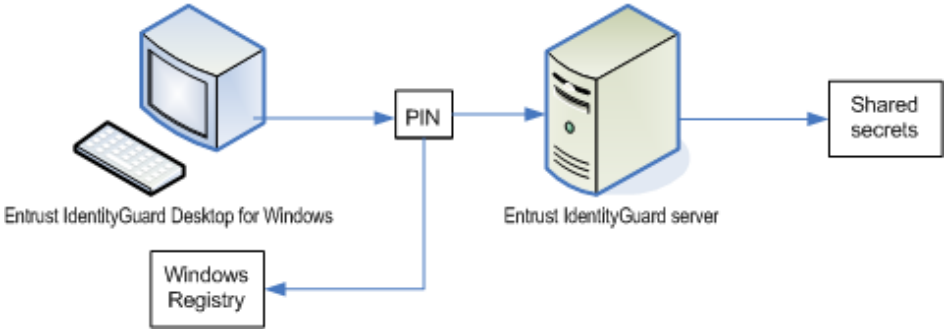
When the user clicks **What is my temporary PIN?**, Entrust Desktop for Microsoft Windows displays a message telling the user how to get a temporary PIN. (See "Using the custom installation wizard" on page 50 for more information about customizing this message.)

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 167.

How the offline temporary PIN works

When a user authenticates to the Entrust Identity Enterprise for the first time, either with a challenge and response or an online temporary PIN, the Entrust Identity

Enterprise Windows Desktop client generates an offline temporary PIN for the user's computer.

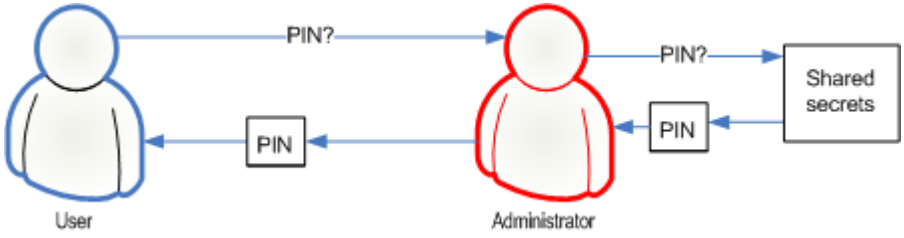


The offline temporary PIN is saved at the Entrust Identity Enterprise Authentication server on the user's **Account Information** page (in the Entrust Identity Enterprise Administration interface) under **Shared Secrets**, and a keyed hash of the PIN is stored in the Windows desktop registry on the user's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

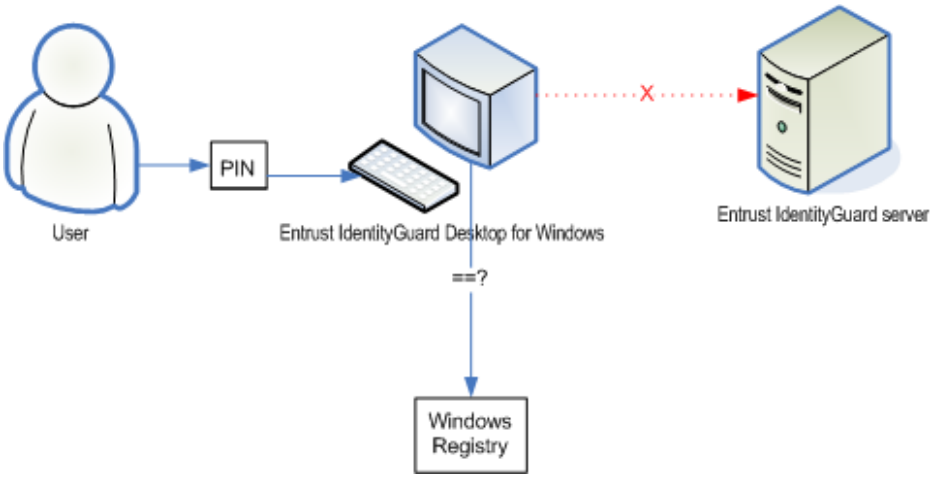
```
IGWOfflinePIN_RLEESP = 2T3D8NPV
```

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 Identity Enterprise Authentication login screen. The user enters the offline PIN into the Entrust Identity Enterprise 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 Identity Enterprise 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 43.

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

Temporary access code

Temporary Access Codes can be used to log in to Identity as a Service when a user cannot access their one-time passcode (OTP), Grid Card, or token authenticator (for example, if a user has misplaced the mobile device containing their Entrust Soft Token mobile application).

Note:
Temporary Access Codes can also be used as a standalone authenticator rather than as a substitute, but Entrust recommends using temporary access codes only for interim authentication.

Temporary access codes can be used to log in to Identity as a Service, OIDC, SAML, or RADIUS accounts. When logging in to Entrust Identity Enterprise applications, they can be used as alternatives for OTP or token authentication but they cannot be used as standalone authenticators.

You can limit the Temporary Access Code to a number of uses or a period of time. For example, you can limit the use of the Temporary Access Code to a single use or a 24-hour period.

Temporary Access Codes are different from one-time passwords (OTP) authenticators. A Temporary Access Code can be used multiple times over a configurable period. An OTP is a single-use authentication code sent to a user's phone, mobile device, or email address during authentication. Temporary Access Codes are not sent to users during authentication.

Administrators must provide the Temporary Access Code to the user. A user is assigned only one Temporary Access Code. If a temporary access code has expired, you must delete it before you can assign a new one to a user.

Users without Entrust

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

For more information, see “Configuring authentication options” on page 43.

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

Note:
Local accounts never require Entrust authentication.

4

Troubleshooting

This section includes information about troubleshooting resources.

Logging

Your installation of Entrust 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 Desktop for Microsoft Windows can write logs to a log file. You enable the logging utility by changing the `EnableedcLogger` and `edcLoggerCompleteFilename` registry settings. For information about these registry settings, see “`EnableEDCLogger`” and “`EDCLoggerCompleteFilename`” on page 207.

Loss of Entrust credential provider after a reboot

After installing Entrust Desktop for Windows and performing a reboot, the user sees only the regular Windows provider and not the Entrust 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 Entrust if not displayed

1. Remove the 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.

Password-less feature does not work for Identity as a Service users

In the CRED_UI scenario, Entrust Credential Provider launches in elevated mode, which restricts the ability to read the password value that is saved in the registry. In this scenario, the password is obtained from the shared secret using the Entrust Identity Enterprise server API. For Identity as a Service users, there is no way to obtain the password because there is no shared secret in the Identity as a Service API; therefore, the password-less feature does not work.

You can enable this feature in one of two ways:

1. **EnablePwdLess** set to `1`, allows the password to be saved in the registry of that machine. Entrust Identity Enterprise and Identity as a Service saves the password using this setting and enables password-less feature in Lock and Unlock scenarios.

   If **EnablePwdLess** is set to `1` and once the user logs into the machine successfully, the password is saved in registry and in Entrust Identity Enterprise (if **SavePwdOnIGServer** is set to `1`). The next consecutive logon allows the user to skip first-factor authentication that is user is not prompted for the password

2. **SavePwdOnIGServer** set to `1`, allows the password to be saved in Entrust Identity Enterprise by passing the password value in the shared secret of the API call. This feature is available only for Entrust Identity Enterprise. With Identity as a Service, there is no shared secret in the API so the password is not saved in Identity as a Service.

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 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_CARD_SUPERSEDED	Entrust authentication was not successful. The grid you are using is no longer active. Please contact your Entrust Identity Enterprise administrator.	The user's grid card is no longer active. Activate or replace the grid card.
IDES_AUTH_INVALID_CHALLENGE	Entrust 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 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 authentication was not successful. You do not have an active grid. Please contact your Entrust administrator.	The user must be assigned an active grid card.
IDES_AUTH_NO_VALID_CARDS	Entrust authentication was not successful. You do not have a valid grid. Please contact your Entrust administrator.	The user must be assigned a valid grid card.
IDES_AUTH_OFFLINE_CHALLENGE_GENERAL_ERROR	Entrust 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.
IDES_AUTH_OFFLINE_CHALLENGE_LOCKOUT	Entrust 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 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.

Table 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_OFFLINE_INVALID_PIN_AND_LOCKOUT	Entrust 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 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 is re-established.
IDES_AUTH_OFFLINE_INVALID_QA_RESPONSE_AND_LOCKOUT	Entrust 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 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.
IDES_AUTH_OFFLINE_INVALID_RESPONSE_AND_LOCKOUT	Entrust 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 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 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.

Table 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_OFFLINE_PIN_LOCKOUT	Entrust 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 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 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 is re-established.	
IDES_AUTH_ONLINE_CHALLENGE_GENERAL_ERROR	Entrust authentication was not successful. Entrust has returned an error. Please contact your administrator.	Entrust has returned a generic error. Check that the Entrust is operational.
IDES_AUTH_ONLINE_INVALID_PIN_AND_LOCKOUT	Entrust 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 administrator.	The user is now locked out because of too many invalid temporary PIN responses.
IDES_AUTH_ONLINE_INVALID_RESPONSE_AND_LOCKOUT	Entrust 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 administrator.	The user is now locked out because of too many invalid responses.
IDES_AUTH_ONLINE_LOCKOUT	Entrust authentication was not successful. You are locked out because you entered an incorrect response too many times.	Please contact your Entrust administrator.

Table 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_AUTH_ONLINE_PIN_GENERAL_ERROR	Your temporary PIN could not be authenticated. Entrust has returned an error.	Please contact your Entrust administrator.
IDES_AUTH_PIN_EXPIRED	Entrust authentication was not successful. The temporary PIN you are using has expired. Please contact your Entrust administrator.	Assign a new temporary PIN to the user, since their current temporary PIN has expired.
IDES_AUTH_PIN_MAX_USES	Entrust authentication was not successful. The temporary PIN you are using has reached maximum uses. Please contact your Entrust administrator.	Assign a new temporary PIN to the user, since their current temporary PIN has reached its maximum uses.
IDES_AUTH_SYSTEM_ERROR	Entrust authentication was not successful. Entrust has returned a system error.	Please contact your Entrust administrator.
IDES_AUTH_USER_NO_CHALLENGE	Entrust authentication was not successful. Please cancel the Entrust authentication dialog and try to login again.	The Entrust Server returned a USER_NO_CHALLENGE error. The user should try and login again.
IDES_CANT_REACH_IG_SERVER	The Entrust Server cannot be reached.	Please contact your Entrust Administrator.
IDES_NO_ACTIVE_TOKEN	Entrust authentication was not performed. You do not have any active tokens.	Please contact your Entrust administrator.
IDES_NO_CHALLENGE_IG_SYSTEM_ERROR	Entrust authentication was not performed. Entrust has returned a system error. Please contact your Entrust Identity Enterprise administrator.	Entrust Server has returned a system error.
IDES_NO_CHALLENGE_OFFLINE_LOCKOUT	Entrust 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 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 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDES_NO_CHALLENGE_ONLINE_LOCKOUT	Entrust authentication was not performed. Your account is currently locked. Please contact your Entrust administrator.	Get challenge set failed due to lockout error.
IDES_NO_CHALLENGE_SET_OFFLINE	Entrust 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 user.
IDES_NO_CHALLENGE_SET_ONLINE	Entrust authentication was not performed. Entrust has returned an error.	Please contact your Entrust 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 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 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 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 5: 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 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 the Entrust server. They must use whatever means are in place in their organization (for example, Entrust Identity Enterprise Self-Service Module) to set up their security questions.
IDES_NO_URL_SETTING	Entrust Authentication was not performed. The Entrust URL setting is missing from the registry. Please contact your Entrust administrator.	There is no Entrust Server URL configured, but Entrust is mandatory.
IDES_NON_IG_USER_OFFLINE	Entrust authentication was not performed. Entrust authentication is mandatory but there are no offline challenges saved for this account. Currently your computer is not connected to the Entrust Server. Please login when the connection is re-established.	The user is a non-Entrust user, or this is the first time the user has logged into Entrust online on this computer, and Entrust authentication is mandatory.
IDES_NON_IG_USER_ONLINE	Entrust authentication was not performed. You are not a registered Entrust user. Please contact your Entrust Identity Enterprise administrator.	The user is a non-Entrust user, but Entrust is mandatory.
IDES_ONLINE_USER_NOT_UNIQUE	Entrust authentication was not performed. Your user name was found in multiple groups. Please contact your Entrust administrator.	If you selected the **Group determined by Entrust Identity Enterprise Server** selection for the group type, this error is displayed if the user is found in multiple groups.
IDES_PVN_CHANGE_INVALID	Entrust authentication was not successful. The new PVN provided was not of appropriate length.	Please contact your Entrust administrator.

Table 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
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 before you can answer a Q&A challenge for later offline use. Please contact your Entrust 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 Entrust server. They must use whatever means are in place in their organization (for example, Entrust Identity Enterprise Self-Service Module) to set up more security questions.
IDES_TOKEN_DRIFT	Entrust authentication was not successful.	Resetting your token may resolve the issue.
IDES_USER_NO_CARD	Entrust authentication was not performed. You do not have any active grids. Please contact your Entrust administrator.	Entrust user does not have a grid card. Entrust is mandatory.
IDES_USER_SUSPENDED	Entrust authentication was not performed. You are currently suspended.	Please contact your Entrust administrator.
IDS_CONFIGURE_QA_FAILURE	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.

Table 5: Windows Login Authentication error messages

Error ID	Error message	Solution or work-around
IDS_NO_SUPPORTED_IG_AUTH_	None of the supported authentication types have been configured for your account. Please contact your Entrust Administrator.	The user must have a grid or token to authenticate to Windows using Entrust.
IDS_OFFLINE_PIN_CUSTOM_MSG	You are trying to authenticate to Entrust in offline mode. An offline temporary PIN can be used to authenticate to Entrust when you do not have the grid you normally use to authenticate, or if you normally use a token to authenticate. Contact your Entrust administrator to receive your offline temporary PIN for this computer.	This help text is displayed when the user clicks **What is my offline temporary PIN?** when logging in offline.
IDS_OFFLINE_QA_MSG	You are trying to authenticate to Entrust in offline mode. You can use Q&A to authenticate to Entrust 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 **How do I use Q&A?** when logging in offline.
IDS_ONLINE_PIN_CUSTOM_MSG	A temporary PIN can be used to authenticate to Entrust when you do not have the grid or token that you normally use to authenticate. Contact your Entrust administrator to receive your temporary PIN.	This help text is displayed when the user clicks **What is my temporary PIN?** when logging in online.

Customizing Entrust Desktop error messages and second factor user-visible text

Credential provider provides a way to customize the error messages listed in Table 4 and user-visible text in the second-factor page based on end user requirement.

To customize the Entrust Desktop error messages\second factor user-visible text

1. Open the file located in `<install_dir>\Entrust\Desktop\1033\edccpenu.xml` for editing in a text editor.
2. To customize the error message for example, `IDES_NON_IG_USER_ONLINE`, search for `IDES_NON_IG_USER_ONLINE` and modify the element text located between the `<value></value>` elements.
3. To customize second-factor user-visible text, search for the string that appears in the second-factor page and modify it. For example, to modify `Cancel` user-visible text in the second factor page, search for `<value>Cancel</value>` and change it to `<value>Return<\value>`.
4. Save and close the file.
5. Logout and log in with valid login credentials. **Return** appears in the second factor screen in the place of **Cancel**.

Known second-factor authentication limitations

In certain authentication scenarios, Microsoft Windows does not call the Entrust Desktop Credential Provider interface leveraged by Entrust Desktop for Microsoft Windows, so second- factor authentication is not performed. Review the details below, and test all authentication scenarios in your environment that are to be protected by Entrust.

Entrust Desktop for Microsoft Windows second-factor authentication is required in the following scenarios:

- Interactive local login (Console Login)
- RDP client login (for example, Microsoft Terminal Services Client (mstsc.exe)
- Unlock scenarios for both Interactive and remote desktop (RDP) client login session

Operations other than those mentioned above should be assumed to be possible without requiring second-factor authentication. For example, the following operations are known to be possible without performing second-factor authentication even when Entrust Desktop for Microsoft Windows is installed:

- Invoking a command as another user (for example, run as command line tool)
- Accessing network shares
- Connecting to another user's existing remote desktop session in a Remote Desktop Services environment

A user is still required to have knowledge of the target user's Windows password, or to have access to other credentials accepted by an enabled credential provider to perform these operations.

5

Customizing the installation package

This chapter contains the worksheets for the **Entrust Desktop Credential Provider Custom Installation** wizard. For details about how to install and configure Entrust Desktop for Microsoft Windows, see “Installing and configuring Entrust Desktop for Microsoft Windows” on page 35

This chapter contains the following sections:

Entrust information worksheet

Use this worksheet to plan the Windows domains and Entrust Identity Enterprise or Identity as a Service Tenant URLs to add when you are installing the Windows Login feature using the **Entrust Desktop Credential Provider Custom Installation** wizard.

Table 6: Entrust Identity Enterprise information worksheet

Windows domain name	Entrust Identity Enterprise /Identity as a Service Tenant 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 Desktop Credential Provider Custom Installation** wizard.

Note:
You can configure only one group type.

Table 7: Configure group type worksheet

Group options	Required (Circle one)
Group determined by Entrust Identity Enterprise	Yes No
Use Windows domain as Entrust Identity Enterprise 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 Desktop Credential Provider Custom Installation** wizard.

Table 8: Configure Windows Login options worksheet

Windows Login options	Required (Circle one)
Authentication to Entrust is mandatory?	Yes No
Authentication to Entrust 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 Desktop Credential Provider Custom Installation** wizard.

Table 9: 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 Identity Enterprise Self-Service Module information worksheet

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

Table 10:

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 Identity Enterprise Self-Service Module URLs to add.

Table 11: Entrust Identity Enterprise Self-Service Module (SSM) information worksheet

Windows domain name	Entrust Identity Enterprise SSM URL(s)

Include additional certification providers worksheet

Use this worksheet to plan the additional certification providers that you want to coexist with Entrust Identity Enterprise Certification Provider. You can add this information to the `AllowCredentialProviders.ini` file to pre-fill this information in the **Entrust Desktop Credential Provider 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 196.

Table 12: 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 Desktop Credential Provider 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 Desktop Credential Provider Custom Installation** wizard.

Table 13: 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 Desktop Credential Provider Custom Installation** wizard.

Table 14: 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)**

6

Registry settings

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

Registry settings can be modified using the custom installation wizard. See Step 24 on page 65 for details.

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

Registry settings under ‘Domains’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\Domains`.

Table 15: Domains registry settings

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

Registry settings under ‘WIGL’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\`.

Table 16: WIGL registry settings

Name	Type	Value
`AllowPasskeyOriginPort`	`REG_DWORD`	This settings allows the origin port to be used for authentication. Set to 0 to use the reverse proxy to expose your Entrust Identity Self-Service Module (SSM) instance on Port 443. Entrust Desktop for Windows requires that Entrust Identity Enterprise passkey authentication is accessible on port 443. The default is `1`. • If the Client origin is hosted in port 443, the Passkey/FIDO2 authentication with configurations A`llowPasskeyOriginPort =0/1` should be successful. • If the Client origin is hosted on port 8445, the Passkey/FIDO2 authentication with configuration `AllowPasskeyOriginPort =1` should be successful, but if `AllowPasskeyOriginPort=0`, it should fail. **Note:** The value must match the value configured under **FIDO2 Passkey Configuration > Passkey Allow Origin Port**. (`igsss.passkey.allow.origin.port`)

Name	Type	Value
AllowPasskeyOriginSubdomain	REG_DWORD	Set to 0 to parse the Entrust Identity Enterprise URL to get replying party ID. Set to 1 to use the relying party ID configured for PasskeyRelyingPartyID key. The default is 0. • If AllowPasskeyOriginSubdomain = 0, the Relying Party ID is taken from the Entrust Identity Enterprise URL and the user must have a Passkey/FIDO2 token with the same Relying Party ID. When set to 0, the PasskeyRelyingPartyID passed in the registry is ignored and Passkey/FIDO2 keys registered on the portal will work with Entrust Desktop for Windows. • If AllowPasskeyOriginSubdomain = 1, the Relying Party ID is taken from the Registry PasskeyRelyingPartyID. All keys registered with PasskeyRelyingPartyID will work with Entrust Desktop for Windows. This value is required only if AllowPasskeyOriginSubdomain = 1. **Note:** The value must the value configured under **FIDO2 Passkey Configuration > Passkey Allow Origin Subdomain**. (igsss.passkey.allow.origin.subdomain)
AuthenticateCredUILogin	REG_DWORD	This registry setting specifies whether to display a **Remember my identity** checkbox on the CREDUI login screen page and to skip second-factor authentication. AuthenticateCredUILogin = 1 EnableRBAAuth = 1 Do not prompt for second-factor in CREDUI Login AuthenticateCredUILogin = 0 EnableRBAAuth = 0 Do prompt for second factor in CREDUI login and do not display **Remember my identity** on the login page.

Name	Type	Value
AuthenticationUnlockDesktop	REG_DWORD	If set to 0, users do not need to perform Entrust authentication when a locked Desktop is unlocked. if set to 1, users need to perform Entrust authentication when a locked Desktop is unlocked The default is 1. This value is set by the configuration wizard in the **Configure Windows Logon Options** page.
AuthenticateLocalUsers	REG_DWORD	This setting allows you to enable or disable Entrust Second-factor authentication for local user logins. This setting applies only for local user logins. Set to 0 to disable Entrust second-factor authentication for local user logins. Set to non-zero to enable Entrust second-factor authentication for local user logins. Default value: If this value is missing, 1 is used as the default. Only administrator user or users of Administrators group can act as an administrator. Set this value to 1 to require multi-factor authentication (MFA) for all local users other than the Administrator.

Name	Type	Value
AuthenticateRDPLogin	REG_DWORD	Allows to you to enable and disable second-factor authentication for RDP client logins. Value 1 - Displays second-factor authentication screen for Domain users (non-admin). Value 2 - Displays second-factor authentication screen for Domain administrator users (users with admin prev.). Value 4 - Displays second-factor authentication screen for Local users (non-admin). Value 8 - Displays second-factor authentication screen for Local administrator users (users with admin privileges). Value 0 - Second-factor authentication screen does not appear for all users. Value 15 - Second-factor authentication screens appears for all users. Default value: 15 Value Range: 0 or 15 (decimal only) The registry setting value can be any combination of above mentioned values. For example: Value of 15 is a combination of all the above values (1+2+4+7). In this example, it displays second-factor authentication for all users (Domain non-admin and admin users and local admin and non-admin users) for RDP logins. This feature can be configured using “Configure options for Windows Login” on page 192 screen of the Entrust Desktop for Windows custom installation wizard. **Note:** This registry setting is created based on the user selection by Entust Desktop for Windows custom installation wizard installer.

Name	Type	Value
AuthenticateRemoteUserAccounts	REG_DWORD	This setting allows you to enable or disable Entrust second-factor authentication for Other Domain user accounts or Remote system user accounts user logins. This setting applies only for remote user accounts (for example, all user accounts other than domain accounts to which the system is tagged to AD Controller or Windows workgroup accounts). Set to 0 to disable Entrust second-factor authentication for remote user accounts. Set to non-zero to enable Entrust second-factor authentication for remote user accounts. Default value: 1 which requires multi-factor authentication (MFA) for all Remote User Accounts users.
CachedLogonUser	REG_BINARY	This registry setting stores cached last logon user details. This registry setting is managed by Entrust Desktop for Windows.
CustomLogoPath	REG_SZ	This registry setting specifies the path to the customized logo image that can be displayed on the login screen.

Name	Type	Value
DisableDisplayLastUserName	REG_DWORD	This setting allows you to configure the display of last successfully logon user name in first factor Log On screen. If set to 0, the name of the last user who logged on successfully appears in the first factor Log On screen. This setting is designed to make logging on faster and easier. If set to 1, the User name field in the first factor Log On screen is blank. This setting enhances system security by not displaying a valid user name. Default value: 0 For remote desktop (RDP) login session, user keys in the user name and password in the RDP client (mstsc tool), the same details appear in the first factor login page based on the setting value. For unlock usage scenarios, both RPD and non-RDP sessions, the user name appears along with user tile similar to windows unlock with group policy (GPO) setting Dontdisplaylastusername=1.
DisableFilter	REG_DWORD	If this setting is missing or is set to 0, the Entrust Credential Provider Filter filters out all other Credential Providers and only the Entrust Desktop Credential Provider is shown. If the value is set to 1, the Entrust 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. **Note**: Do not change this setting unless required.
DisableSSLRevocationChecking	REG_DWORD	If the setting is missing or the value is set to 0, the revocation status of the SSL certificate is checked. If the value is set to 1, the status of the SSL certificate is not checked. This value is not set by the configuration wizard.

Name	Type	Value
DontDisplayLockedUserId	DWORD	Set the registry setting value to 1 to hide username in the first-factor lock screen only. Set the registry setting value to 2 to hide the username in second-factor lock screen only. et the registry setting value to 3 to hide the username in both first and second factor lock screen. Set the registry setting value to 0 to display the username in both the first and second-factor lock screen. If the setting is missing, the default value 0 is used.
EDCLoggerCompleteFilename	REG_SZ	This setting specifies the name of the log file. By default the file is: C:\EDCLogger.log
EDCLoggerFileSizeForRollOn	REG_DWORD	This setting specifies the rollover size. If the log file size reaches the configured file size, the log files are rolled over. 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. The default is 2 MB
EDCLoggermaxBackupindex	REG_DWORD	This setting specifies the maximum log files backed up with a rollover. Allowed values are 0-99. A value greater than 99 defaults to 99. Set to 0 to disable log file rollover. The default is 5

Name	Type	Value
EDCTitle	RG_SZ	This registry key allows you to configure the title for the login screen. Default value: " "(Blank). No title appears on the Login screen. Value: Type any string you want to appear on the first-factor and second-factor Login screens. If this is not present (missing or deleted), Entrust Desktop for Windows displays a message box title with a Logon screen title, Entrust. It is located under <install folder>\Desktop\1033\edccpenu.xml with data name IDS_MESSAGE_BOX_TITLE.
EnableCombinedAuth	REG_REG_SZWORD	Set to 0 to disable CombinedAuthentication. Set to 1 to enable CombinedAuthentication. When set users can authenticate using, grid, token, or Mobile TVS authentication. The default is 0. This feature complies with the Payment Card Industry (PCI) Data Security Standards (DSS). For more information, see https://www.pcisecuritystandards.org.
EnableCombinedAuthDomainList	REG_SZ	Users can enable the combined authentication for specific domains using this registry. To do the domain names separated by semi colon (;) to this registry entry. If this setting is not present in the registry or if the value is empty, then all the domains are protected by the Combined Authentication.

Name	Type	Value
EnableMachineAuthIDG	REG_DWORD	EnableMachineAuthIDG = 1 If Enablemachineauthentication is selected during Entrust Identity Enterprise installation, then the following two registries get created in Entrust Desktop for Windows with the following values: • EnableRBAAuth with the value set to1. • EnableMachineAuthIDG with the value set to 0. If machine authentication is configured in Entrust Identity Enterprise, set EnableMachineAuthIDG = 1. If machine authentication not is configured in Entrust Identity Enterprise, set EnableMachineAuthIDG = 0.
EnableOffnetworkPwdReset	REG_DWORD	Specifies whether the "Forgot password?" link appears to users on thelogin page and allows a domain user to reset their password even if the computer is not connected to corporate network. Set to 1 to display the "Forgot password?" link on a user's login page. If the value is set to 0, the link does not appear on the user's login page. The link does not appear if Enablepwdreset is 0 and EnableOffnetworkPwdReset is 0. Default value: 0
EnablePwdReset	REG_DWORD	This registry setting specifies whether the "Forgot password?" link appears to users on login page. Set to 1 to display the "Forgot password?" link on a user's login page. If the value is set to 0, the link does not appear on the user's login page. Default value: 0

Name	Type	Value
EnableEDCLogger	REG_DWORD	If the value is set to 0, logging is disabled. If the value is set to 1, logs are written to file. Logging is disabled by default. **Note**: Logging should only be enabled for troubleshooting or if requested by Entrust support. Disable troubleshooting when it is no longer required.
EnablefallbackAuthentication	REG_DWORD	EnableFallbackAuthentication = 1 If push authentication is not successful, the user should fallback to the next authenticator if more than one authenticator is set in the resource rule or be redirected to the first-factor page if only Mobile push authenticator is set in resource rule. EnableFallbackAuthentication = 0 If push authentication is not successful, the user is prompted with Retry and Cancel options. **Retry** - A new challenge is sent to the user. **Cancel** - Redirects to next authenticator if more there is more than one authenticator set in the resource rule or to the first-factor page if only Mobile push is set.
EnableFIDO2Registration	REG_DWORD	If Enable FIDO2Registration is 1, register Passkey/FIDO2 appears on the second-factor screen of Entrust Desktop for Windows. If EnableFIDO2Registration is 0, register Passkey/FIDO2 does not appear on the second-factor screen of Entrust Desktop for Windows.
EnableManualOTP	REG_DWORD	If set to 0, OTP is delivered automatically to the user's contact information. If set to 1, OTP is available by contacting the Entrust administrator. Default is 0.

Name	Type	Value
EnableOfflineQA	REG_DWORD	If set to 0, offline question and answer (Q&A) is disabled. Users are unable to see the Q&A interface and are not able to use Q&A to authenticate when the Entrust Server is unreachable. If set to 1 offline (Q&A) login is enabled. Default is 1. This value is set by the configuration wizard in the **Configure Windows Logon Options** page.
EnableOnlineTempPINAuth	REG_DWORD	This registry setting specifies whether the **Use temporary PIN** link is displayed to users. If the value is set to 1, the **Use temporary PIN** 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. If the value is set to 0, the link is not displayed on the second-factor login page. Default value: 1
EnableOfflineTempPINAuth	REG_DWORD	Set to 0 to disable offline temporary PIN if a user fails to connect to Entrust Identity Enterprise Server. If set to 1, the temporary PIN is enabled. The default is 1.
EnablePwdMask	REG_DWORD	Set to 0 to enable password reveal. (The user will need to click on the eye symbol in the password text box.) Set to 1 to disable password reveal. The default is 0.
EnablePwdless	REG_DWORD	Set to 1 to enable the passwordless. When set, if the user is also an Entrust 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.

Name	Type	Value
EnableRBAAuth	REG_DWORD	Use this setting for risk-based authentication. Default: 0 (disabled) Enable RBA: 1
EnableTVS	REG_DWORD	Set to 1 to allow a user with a full UPN name to perform second0factor authentication, then log in. Set to 0 to not allow a user with full UPN name to perform second-factor authentication and then log in. The default is 0.
EnableUPNUserName	REG_DWORD	If set to 1, the entire UPN name is considered as the user ID for second-factor authentication. If you do not have a user in the back end with a UPN as the userID (or UPN as the alias) and the user tries to enter their userID in UPN format, they are not prompted for second-factor for IGAuthenticationMandatory = 0. If set to 0, the user ID portion of the UPN name is considered as the user ID ffor second-factor authentication The default is 0.
FaceAuthentication Timeout	REG_DWORD	No of attempts to retry Face authentication after 5 seconds. This registry key is applicable for Face Biometric authentication. Value: Positive decimal value Default: 25 For example, if the value is set to 20, Entrust Desktop attempts to authenticate using Face Biometric 20 times after every 5 seconds. In this example, the user can access the second-factor (Face Biometric authentication) page for a maximum of 100 seconds after which Entrust Desktop for Microsoft Windows will fallback to the first factor page from the Face Biometric authentication page on timeout.

Name	Type	Value
Group	REG_SZ	This value specifies the user's group. If both this setting and **UseWindowsDomainAsGroup** are used, this value takes precedence. This value is set by the configuration wizard in the **Configure Group Type** page.
HTTPConnectTimeLimit	REG_DWORD	Time limit in seconds for connecting to the Entrust Identity Enterprise Server. If this value is missing, a value of 10 seconds is used. This value is not set by the configuration wizard.
HTTPReceiveTimeLimit	REG_DWORD	Time limit in seconds for connecting to the Entrust Identity Enterprise Server. If this value is missing, a value of 10 seconds is used. This value is not set by the configuration wizard.
HTTPSendTimeLimit	REG_DWORD	Time limit in seconds for connecting to the Entrust Identity Enterprise Server. If this value is missing, a value of 10 seconds is used. This value is not set by the configuration wizard.
IGAuthenticationMandatory	REG_DWORD	If this value is set to 0, unregistered users can access this computer If this value is not set to 0, only users registered on Entrust can access this computer. This value is set by the configuration wizard in the **Configure Windows Logon Options** page
LogonTo	REG_SZ	Specifies whether the last login was on the local computer or on the domain.
LogonType	REG_DWORD	Set to 3 for the default log on type intended for high performance servers to authenticate users. If set to 2 for a system where the group policy to restrict network logins is enabled. This log on type is intended for users who will be interactively using the computer. The default value is 3.
LogonUser	REG_SZ	Contains the name of the last user to log in.

Name	Type	Value
OfflineChallengeAttemptsAllowed	REG_DWORD	The maximum number of allowed failed grid login attempts. after which the user is locked out of the computer. If this value is missing, 5 is used. This value is set by the configuration wizard in the **Configure Windows Offline Options** page.
OfflineChallengeResponseCount	REG_DWORD	The number of challenge responses saved for offline authentication. If this value is zero or missing, 5 is used. This value should not be changed.
OfflineLockOutTime	REG_DWORD	The offline temporary PIN lock-out time limit in minutes. If this value is set to zero or missing, 15 minutes is used. This value is set by the configuration wizard in the **Configure Windows Offline Options** page.
OfflineOTPDownloadHours	REG_DWORD	If set to 0, offline token authentication is disabled. Set the lifetime (in hours) that Entrust Desktop for Windows allows offline token authentication, as follows: • For Entrust Identity Enterprise, set a decimal value between 1 and 720. • For Identity as a Service, set a decimal value between 1 and 336. This value is set by the custom installation wizard in the **Configure password-less and offline Token authentication options** page.
OfflineOTPMaxTimeSteps	REG_DWORD	The number of time steps that are searched to find a matching user response during offline authentication. This is an optional configuration. This optional key can be configured using the Custom Installation wizard **Specify Additional Registry Values** page. This value is relative to laptop or computer time drift. For 1 minute time drift, a value of 4 needs to be configured. For example, for a 5 minute time drift, the value of OfflineOTPMaxTimeSteps should be set to 20 (5*4).

Name	Type	Value
OfflineQAAttemptsAllowed	REG_DWORD	The maximum number of allowed failed Q&A login attempts after which the user is locked out of the computer. If this value is missing, 5 is used. This value is set by the configuration wizard in the **Configure Windows Offline Options** page.
OfflineTemporaryPINAttemptsAllowed	REG_DWORD	The maximum number of allowed failed temporary PIN login attempts after which the user is locked out of the computer. If this value is missing, 5 is used. This value is set by the configuration wizard in the **Configure Windows Offline Options** page.
OfflineTempPINMessage	REG_SZ	Customizable string displayed in a message box that tells users what an offline temporary PIN is and and how to get one. The default message is: `You are trying to authenticate to Entrust Identity Enterprise in offline mode. An offline temporary PIN can be used to authenticate to Entrust Identity Enterprise when you do not have the grid you normally use to authenticate, or if you normally use a token to authenticate. Contact your Entrust Identity Enterprise administrator to receive your offline temporary PIN for this computer.` An alternate message can be set in the **Configure Windows Offline Options** page of the configuration wizard.

Name	Type	Value
OfflineTokenThreshhold	REG_DWORD	Once the user has downloaded the offline token through risk-based authentication, subsequent logins display the remaining validity of the offline token. If the remaining validity is equal to or less than the threshold defined in the OfflineTokenThreshold registry, the user is directed to a high-risk authentication flow where token or a token push is presented as the first challenge in the second-factor authentication. **Note:** The OfflineTokenThreshold registry setting applies exclusively to Token and Token Push authentication methods. It is not applicable to other types of authenticators. The Offlinetokenthreshold functionality works only when the system is connected to the network and not in offline mode. **Example**: If OfflineOTPDownloadHours is set to 168 hours (7 days) and **OfflineTokenThreshold** is set to 72 hours (3 days) then the user will be navigated to high-risk at the 96-hour (4th day) to download again the offline tokens.
OffnetworkPwdResetCacheRemiderTime	REG_DWORD	Numeric value in minutes ranging from 1 to 129600 (90 days in minutes). The default value for password caching notification reminder time which appears in the installer screen is 1 week, for example:7 *24*60= 10080 mins. Password caching reminder notification time in minutes after which a reminder alert message appears asking the user to connect to organization's corporate network to cache Windows Login password. This message appears when the user logs in to the system after they reset their password in off-network mode until the user connects and caches Windows Login password.

Name	Type	Value
`OnlineTempPINMessage`	`REG_SZ`	Customizable string displayed in a message box telling users what a temporary PIN is and how to get one. The default message is: `A temporary PIN can be used to authenticate to Entrust when you do not have the grid or token that you normally use to authenticate. Contact your Entrust administrator to receive your temporary PIN.` An alternate message can be set in the **Configure Windows login Options** of the configuration wizard.
`PasskeyRelyingPartyID`	`REG_SZ`	This setting allows Entrust Desktop for Windows to configure the relying party ID for Passkey/FIDO2 authentication. It can be either a single host or any host that belongs to a domain or associated subdomains. A given passkey can only be used to authenticate to the origin of the relying party to which it originally registered. Possible values: Can be blank if `AllowPasskeyOriginSubdomain =0` or `hostname/domain/sub-domain`. Default value: `Blank` **Note:** The value must match the value configured under **FIDO2 Passkey Configuration > Passkey Relyaing Party ID**. (`igsss.passkey.allow.relying.party.id`)

Name	Type	Value
PushAuthenticationTimeout	REG_DWORD	No of attempts to retry Push authentication after 5 seconds or authenticate using a token on timeout. This registry key is applicable for both mobile smart credentials and Token push. Value: Positive decimal value Default: 10 For example, if the value is set to 15, Entrust Desktop attempts to authenticate using push for 15 times after every 5 seconds (in this example, the user can access the second-factor (push authentication) page for a maximum of 75 seconds after which Entrust Desktop for Microsoft Windows will fallback to either the token authentication page from the Token push authentication page or the first factor page from the mobile smart credential push authentication page on timeout.
UseCustomLogo	REG_DWORD	Specifies whether to use a custom logo.
UseIntelliTrustServer	REG_DWORD	If set to 0, users authenticate using Entrust Identity Enterprise Server. If set to 1, users authenticate using Identity as a Service. Default: 0
UseWindowsDomainAsGroup	REG_DWORD	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. This value is set by the configuration wizard in the **Configure Group Type** page.

Name	Type	Value
UsersExemptedOfflineAuth	REG_SZ	In offline mode configurable 2FA exempt Domain Account for Entrust 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. To enable this feature add a registry key UsersExemptedOfflineAuth under HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL, then add the below string key pair <name/value> under this key. Name: Domain name Type: String Values: User names exempted from offline 2FA separated by semicolon.

Registry settings under ‘DomainsAlias’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\DomainsAlias`.

Domain alias creates additional domain names that would point to one domain for Desktop Credential Provider login purposes. For example, if your short domain name is `testdomain` (for example, i`g.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 17: DomainsAlias registry settings

Name	Type	Value
`<name of the domain alias>` `For example: test4`	`REG_SZ`	This setting specifies the domain name the alias points to. This value should be one of the key names mentioned under registry key, as follows: For Entrust Identity Enterprise, `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\Domains` For Identity as a Service, `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\IDaaS\Domains` For example, the short domain name for `ig.testdomain.com` is `testdomain`. In this example, the domain alias name is resolved as `testdomain`. This optional registry key can contain one or more key-value pairs.

Registry settings under ‘AllowCPs’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\AllowCPs`.

Table 18: 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 Desktop.

Registry settings under ‘SSM’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\SSM`.

Table 19: SSM registry settings

Name	Type	Value

`AllowedURL Suffixes`	REG_SZ	A list of custom or additional SSM URLs that you want to make available to the Entrust Desktop client. URLs must be separated by a semi-colon.
		
		The specified URLs will be available to users through the self-service link on the Windows login screen. See “Enabling other self-administration operations, in addition to password reset” on page 232 for details.
		
		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 “List of default URLs that are accessible by clicking the self-service link on the Windows login screen” on page 233.
		
		The URL specified here will be appended to the end of the main Self-Service Module URL (for example, https://example.com:8445/IdentityGuardSelfService).
		
		Only URLs ending in the specified string (and terminated with a “?” or a “;”) will be allowed.
		
		Example:
		
		If `AllowedURLSuffixes` is set to:
		
		`administer/myresetToken`
		...then the Desktop client can access:
		
		`https://ssmhost.example.com:8445/IdentityGuardSelfService/administer/myresetToken?query1=abc`
		
		...and:
		
		`https://ssmhost.example.com:8445/IdentityGuardSelfService/administer/myresetToken;JSESSIONID=123465346DF321`
		...but not:
		
		`https://ssmhost.com:8445/IdentityGuardSelfService/administer/myresetToken/RemainingURL/url?query1=abc`

Name	Type	Value
`DisallowedURLSuffixes`	REG_SZ	The same as `AllowedURLSuffixes`, except that this list contains URLs that users are *not* allowed to access through the self-service link on the Windows login screen. 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 "List of default URLs that are accessible by clicking the self-service link on the Windows login screen" on page 233. For example, if you want to disallow this URL (which is allowed by default)... `<SSM_URL>/administer/lostToken` ...then add `<SSM_URL>/administer/lostToken` to `DisallowedURLSuffixes`.
`InitialURLSuffix`	REG_SZ	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). If the value is "/", the SSM Self-Administration Actions page is used. 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. For details on customizing the self-service link, see "Enabling other self-administration operations, in addition to password reset" on page 232.

Registry settings under ‘SSMDomains’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\SSMDomains`.

Table 20: 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 21: Credential Providers registry settings

Name	Type	Value
`ProhibitFallbacks`	`REG_DWORD`	Set this value to 1 to prevent users from circumventing the requirement to log in with second-factor Entrust credentials by re-booting in Safe Mode. 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 second-factor credentials. By default, Microsoft only runs Microsoft Credential Provider when starting in Safe Mode. The default setting is 0. **Attention**: By setting this registry key, you will explicitly override the fallback safety mechanism that Windows supplies to troubleshoot configuration errors and malfunctioning Credential Providers. Users may be blocked from login in the event of Credential Provider failure.

Registry settings under ‘IDaaS\Domains’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\IDaaS\Domains`.

Table 22: IDaaS domain registry settings

Name	Type	Value
`<domain name>`	`REG_RZ`	URL of Identity as a Service. For example: `https://<tenantname>.<region>.trustedauth.com` This value is set by the configuration wizard in the **Specify Identity as a Service Server** page.

Registry settings under ‘IDaaS\AppId’

Located in `HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\WIGL\IDaaS\AppId`.

Table 23: IDaaS AppId registry settings

Name	Type	Value
`<domain name>`	`REG_RZ`	Application ID of the application in Identity as a Service. For example: This value is set by the configuration wizard in the **Specify Identity as a Service Server** page.

7

Entrust Desktop client integration with SSM

This appendix contains information about integrating the Entrust Desktop client with Entrust Identity Enterprise Self-Service Module. This integration allows Entrust 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 Desktop client with the Self-Service Module.

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

Upgrade to the latest version, as documented in "Preparing for installation" on page 36. 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 231.

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 232.

If you are currently running Entrust Desktop 13.0, and you must customized the default Self-Service URLs, as follows:

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 233.
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 Follow the procedure "Installing for Entrust Identity Enterprise" on page 67.

   For details on the `AllowedURLSuffixes` registry setting and other Self-Service Module-related registry settings, see "Registry settings under 'SSM'" on page 222.

   For details on enabling password reset and other self-service options, see "Enabling other self-administration operations, in addition to password reset" on page 232.
3. Uninstall the old version from the users' desktops.
4. Re-install the new installation package that includes your custom URLs.
5. Apply Entrust Desktop 13.0 for Microsoft Windows to users' desktops.

Enabling Active Directory password reset

You can enable users of the Entrust 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 "Installing for Entrust Identity Enterprise" on page 67.
2. 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 40).

   The password reset link in your Entrust Desktop client will allow users to reach the URLs listed in "Password reset URLs:" on page 233.

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 231). 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 Follow the procedure "Installing for Entrust Identity Enterprise" on page 67.
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 Entrust Desktop client.
3. Continue through the procedure and follow the instructions 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 199.
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 222.

   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/validateSecondFactorAuthentication`
- 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
```

Index

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

C

D

E

F

G

H

I

L

M

O

P

R

S

T

U

W